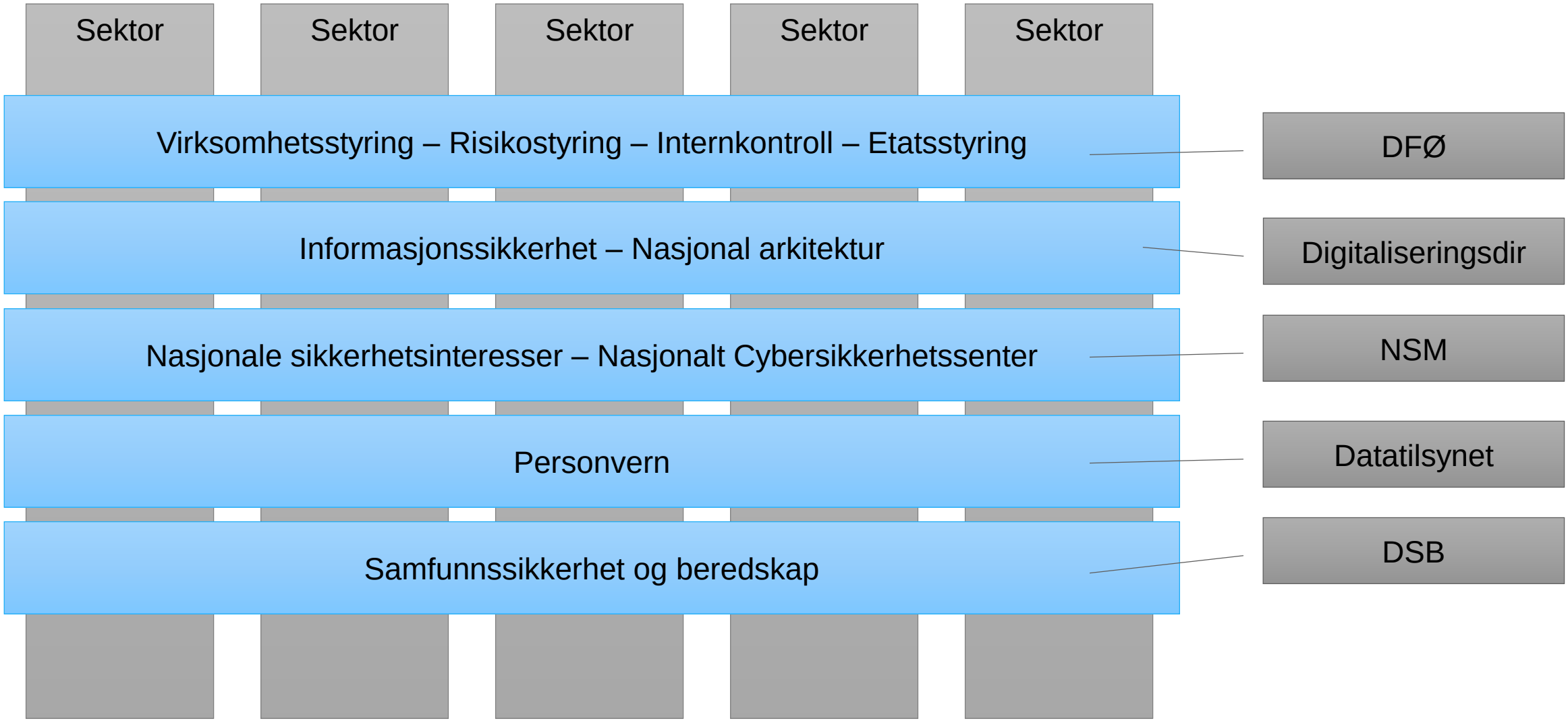
Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

# Sammenhenger Digitaliseringsdirektoratet – DFØ – NSM

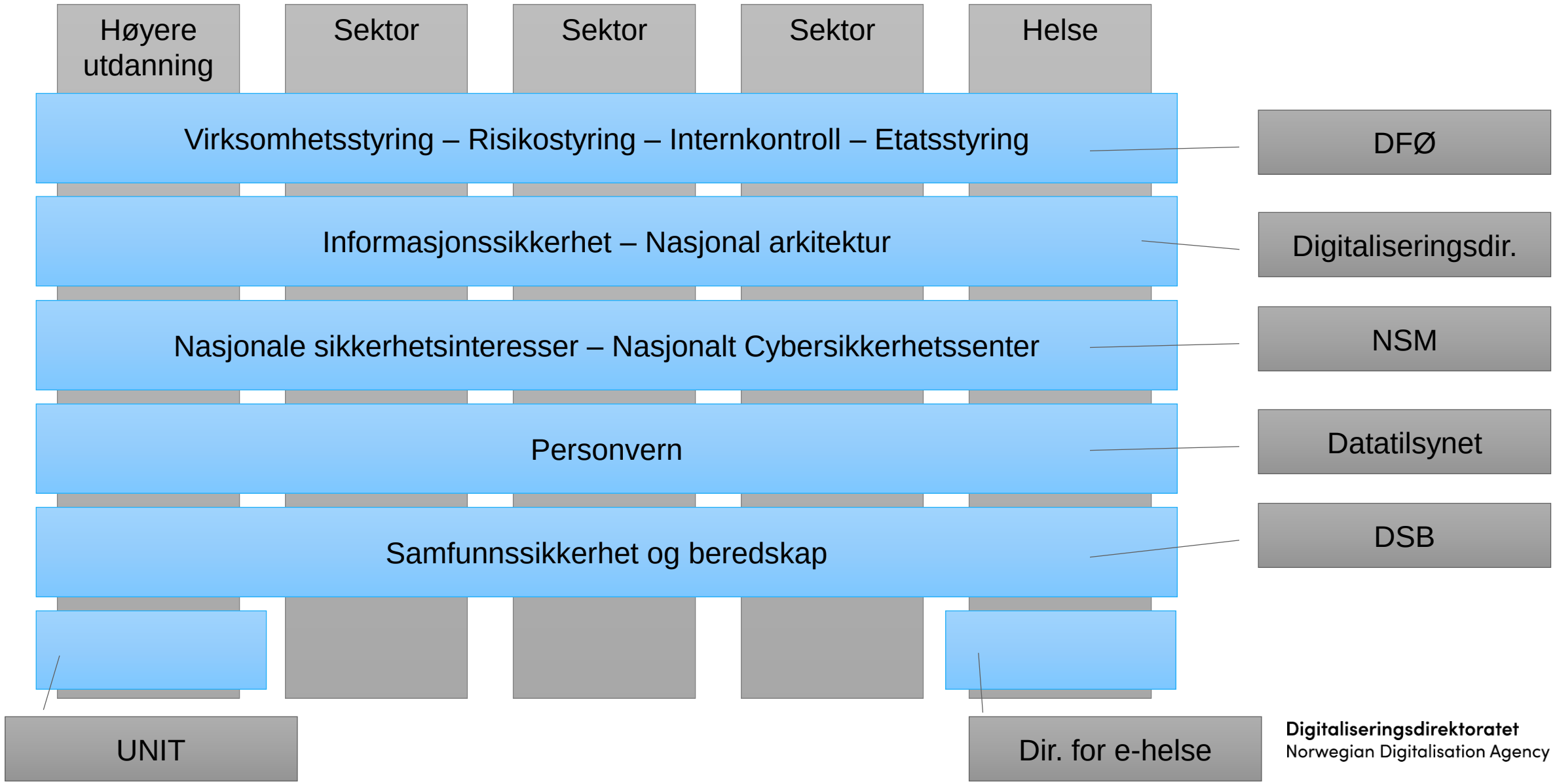
–

Katrine Aam Svendsen
Seniorrådgiver
NIFS 04.02.2020

# Infosikkerhet på tvers og på langs



# Infosikkerhet på tvers og på langs




Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

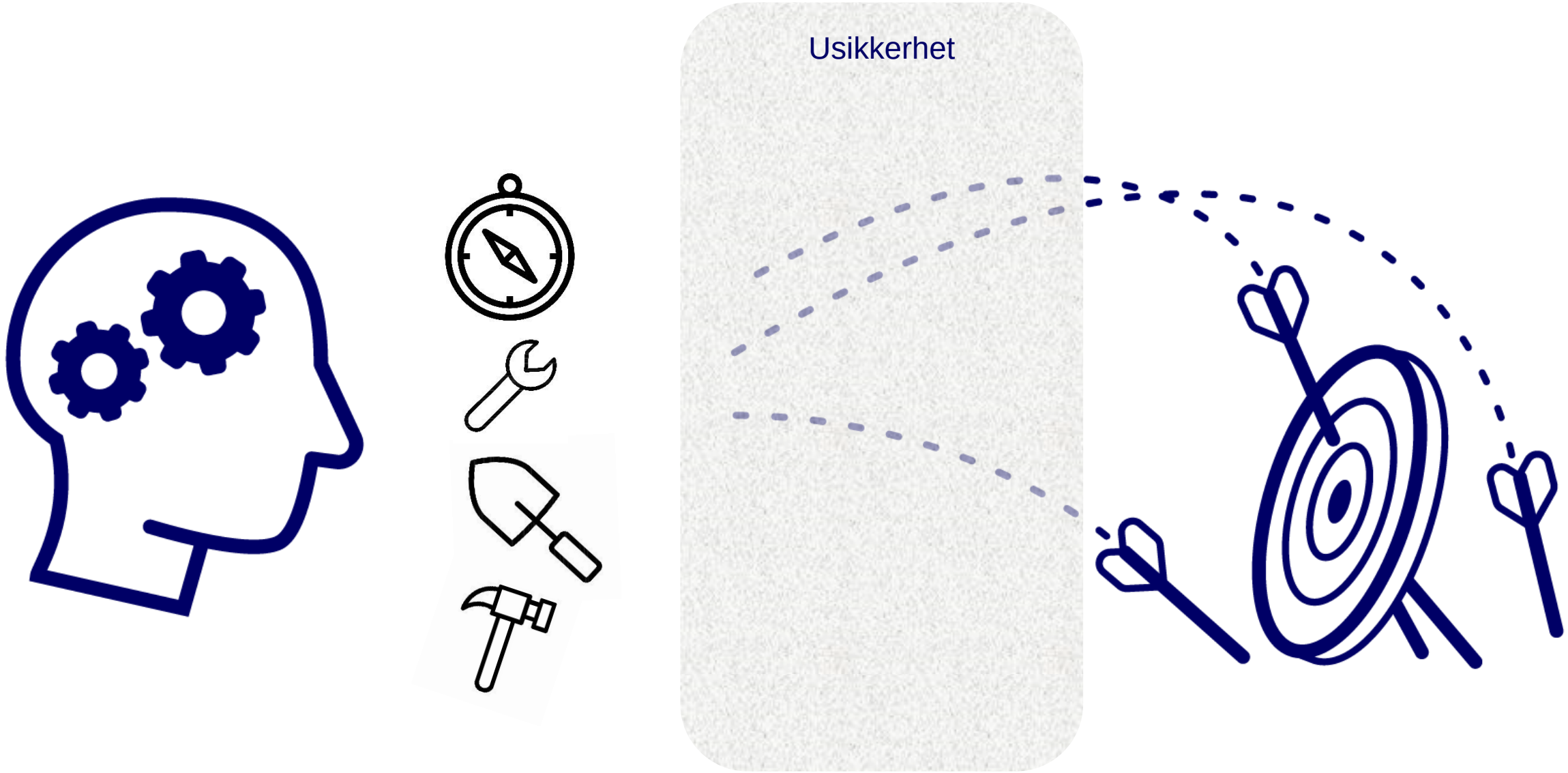
# «Leseveiledning»…

# Digitaliseringsdirektoratets veiledning på internkontroll (styring og kontroll) på informasjonssikerhetsområdet etter eForvaltningsforskriftens §15

# DFØs veiledning på internkontroll etter økonomiregelverket i staten

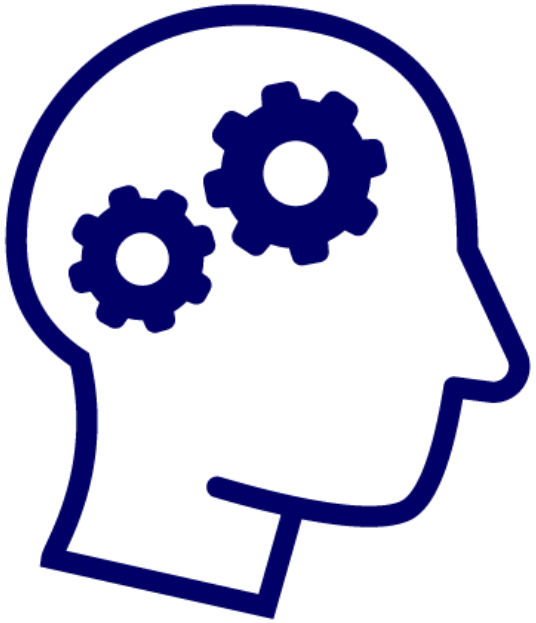
**Direktoratet for forvaltning og økonomistyring**

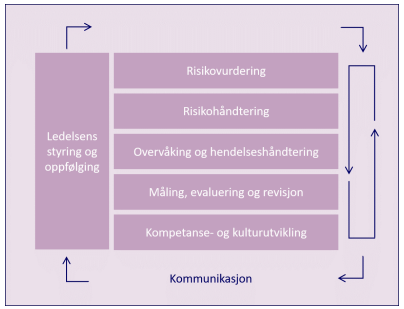
# NSMs veiledning på sikkerhetsstyring etter sikkerhetsloven og virksomhetsikkerhetsforskriften

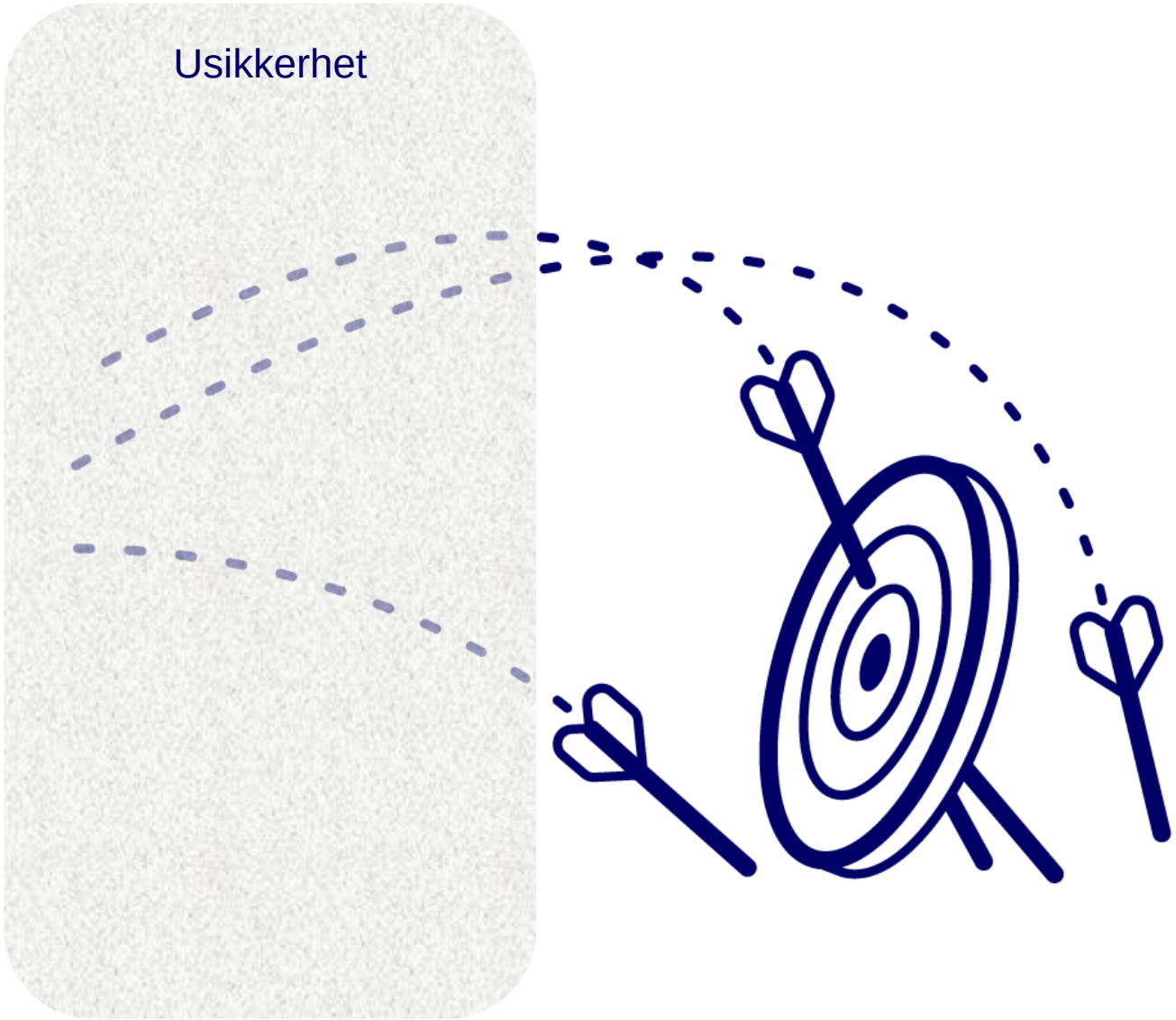



Risiko: Virkning av usikkerhet knyttet til mål (NS-EN ISO/IEC 27000)

# Styring og kontroll

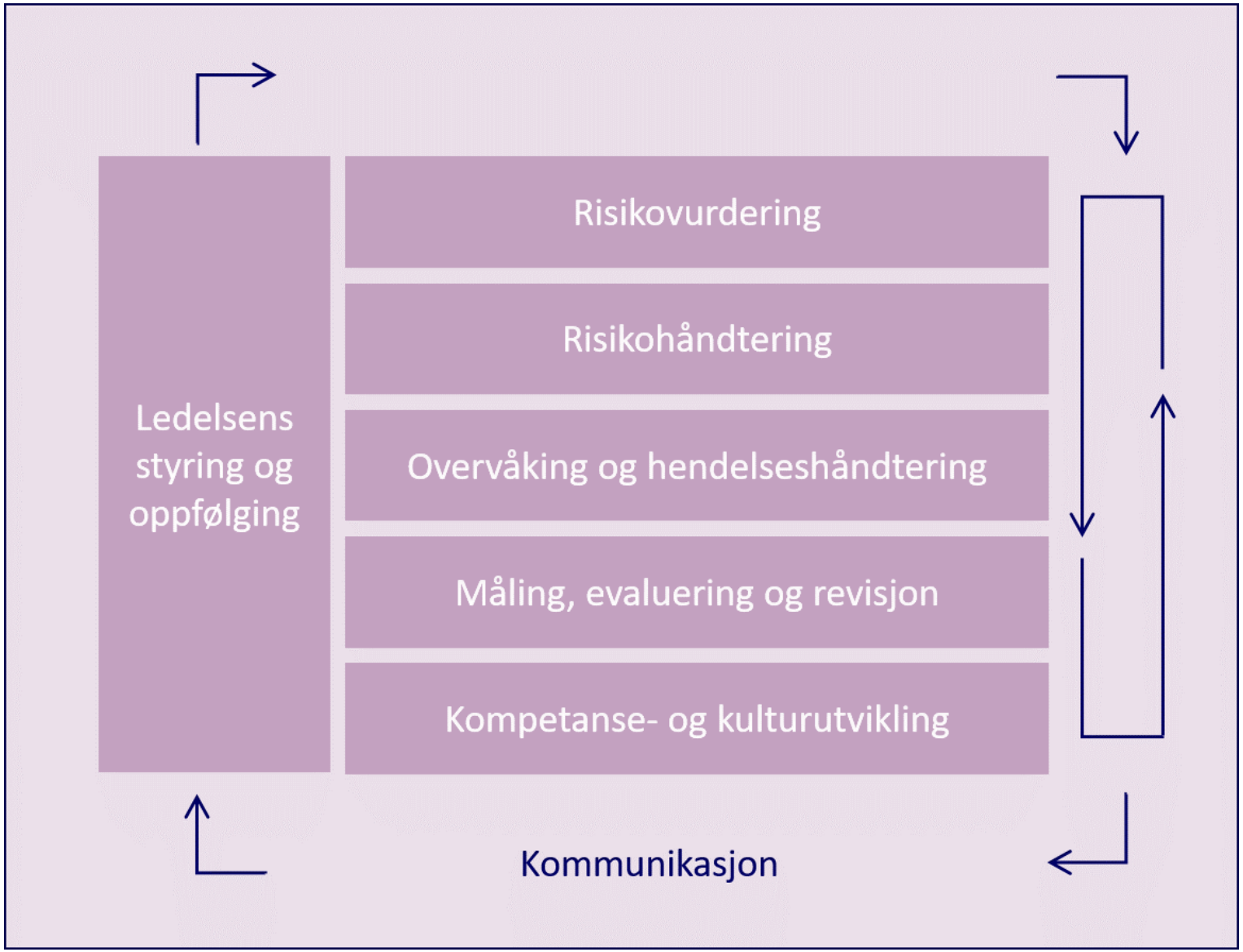





Risiko: Virkning av usikkerhet knyttet til mål (NS-EN ISO/IEC 27000)

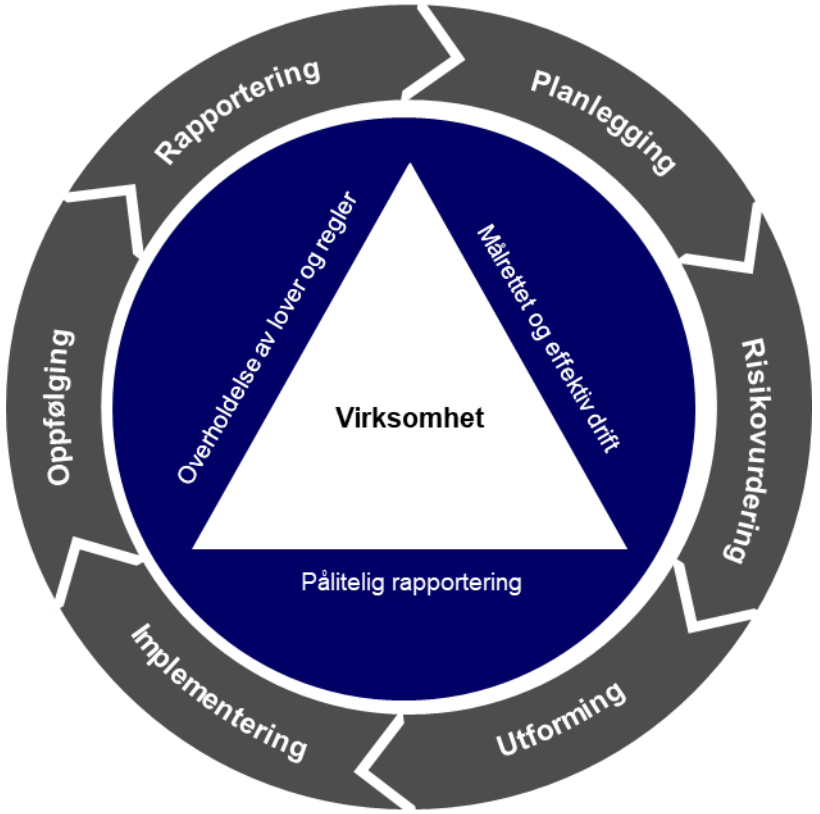
# Internkontroll - informasjonssikkerhet




# Hva er internkontroll?

Internkontroll er en **prosess**, gjennomført av virksomhetens **ledelse** og **ansatte,** som er utformet for å gi **rimelig sikkerhet** vedrørende måloppnåelse innen følgende områder:

- *Målrettet og effektiv drift*
- *Pålitelig rapportering*
- *Overholdelse av lover og regler*



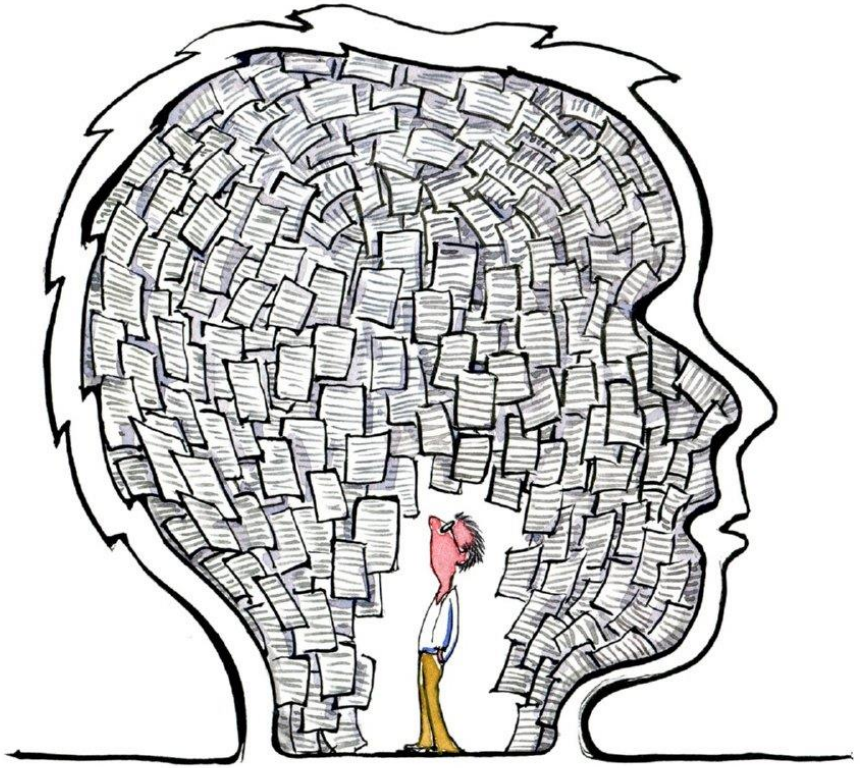

Systematisk gjennomføring av de seks stegene i internkontrollprosessen bidrar til å oppfylle de tre internkontrollmålsettingene og **kontinuerlig forbedring** i virksomheten.

**Direktoratet for forvaltning og økonomistyring**

# Hva er sikkerhetsstyring?

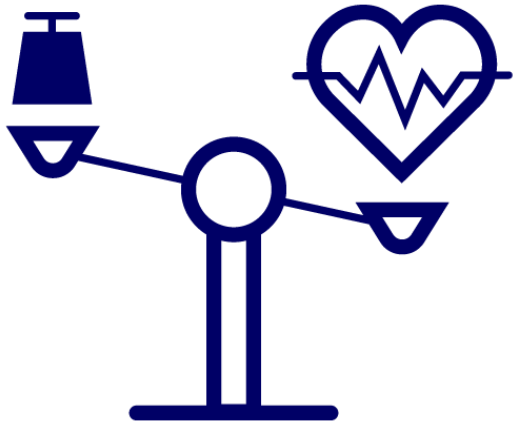
- Systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå.

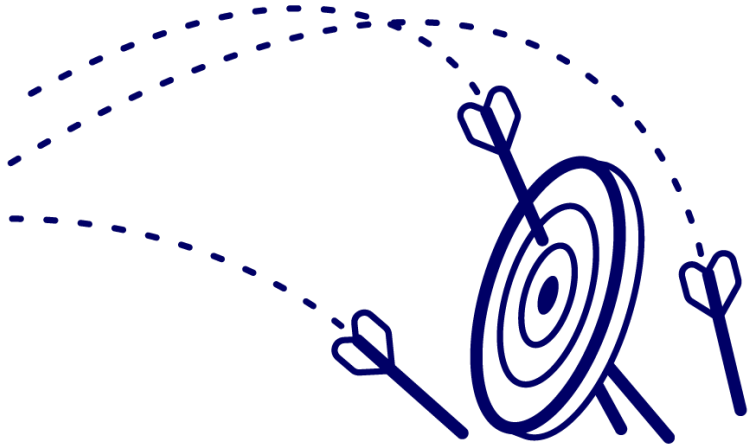
- Et styringssystem for sikkerhet skal inneholde:
  - Sikkerhetsledelse
  - Sikkerhetsorganisering
  - Risikostyring
  - Sikkerhetstiltak
  - Forhold til andre virksomheter
  - Sikkerhetsoppfølging
  - Sikkerhetsdokumentasjon



# Fellestrekk – internkontroll/styring og kontroll/ sikkerhetsstyring

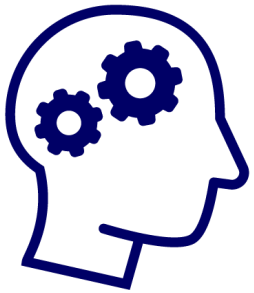
Systematiske aktiviteter

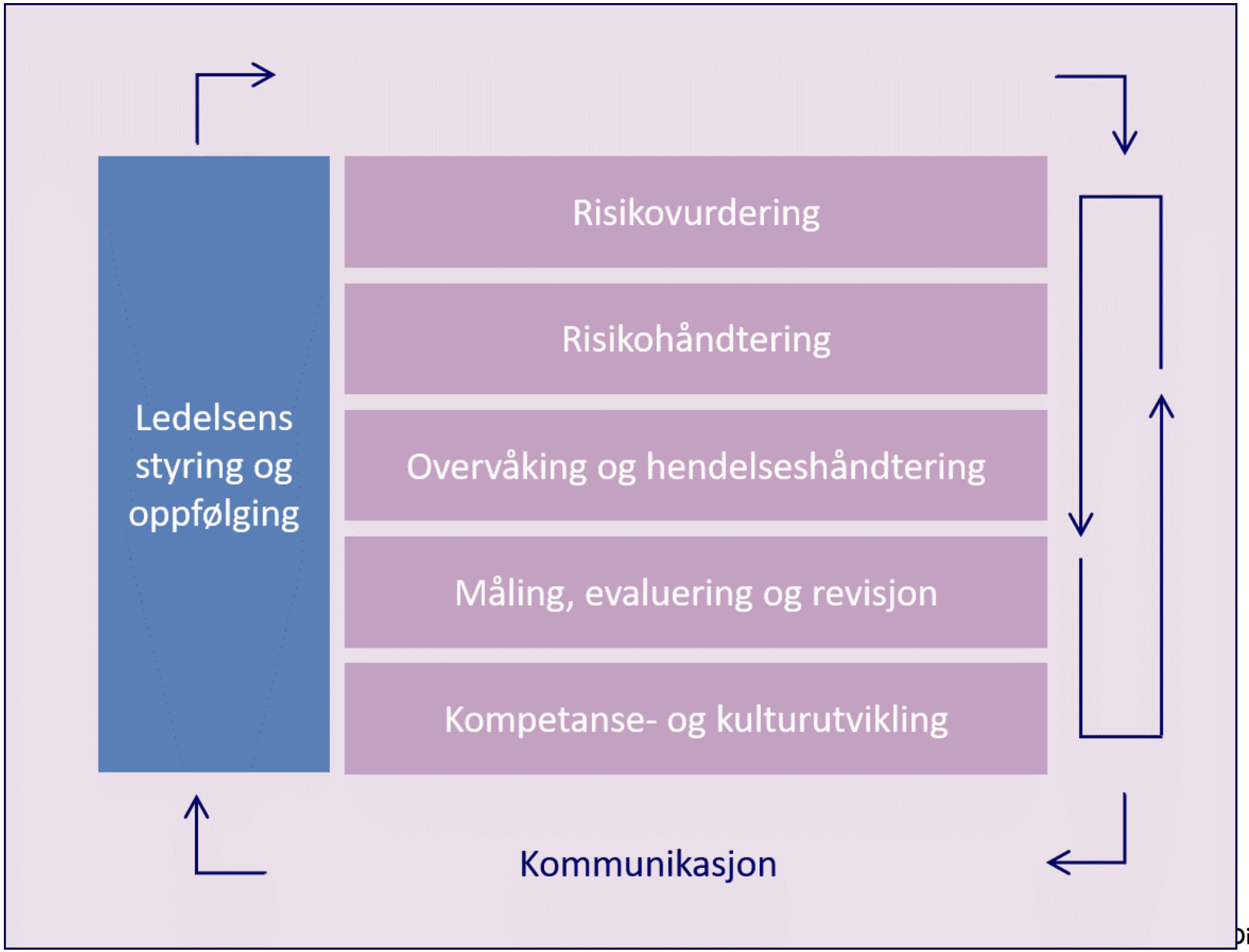




Rimelig sikkerhet – tilpasset – forsvarlig

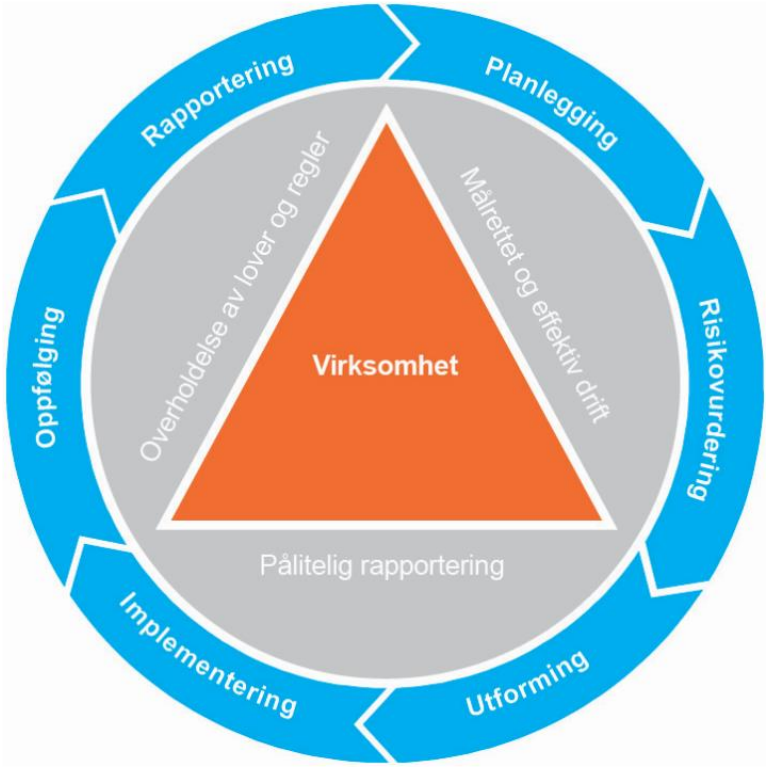
# Ledelse og styring…




Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

# Lederansvar og styring

- Leder har ansvar for at virksomheten har etablert en effektiv internkontroll, og at denne gjennomføres og fungerer på en tilfredsstillende måte.
- Internkontroll er et lederansvar, og er en nødvendig forutsetning for god styring.
- Leder har ansvar for at virksomheten har etablert et fundament for internkontrollen.

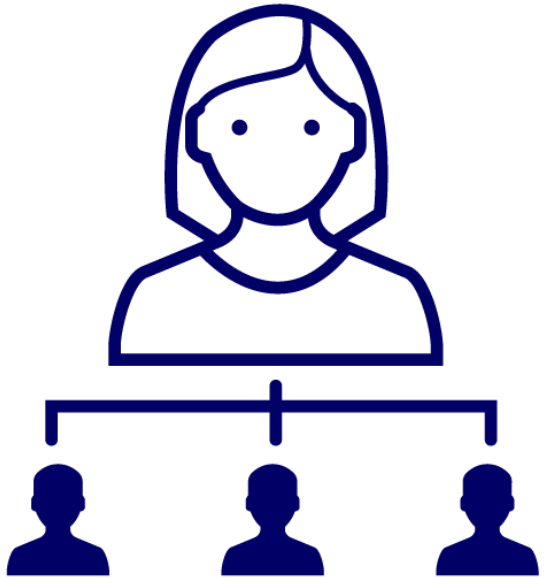


# Sikkerhetsledelse

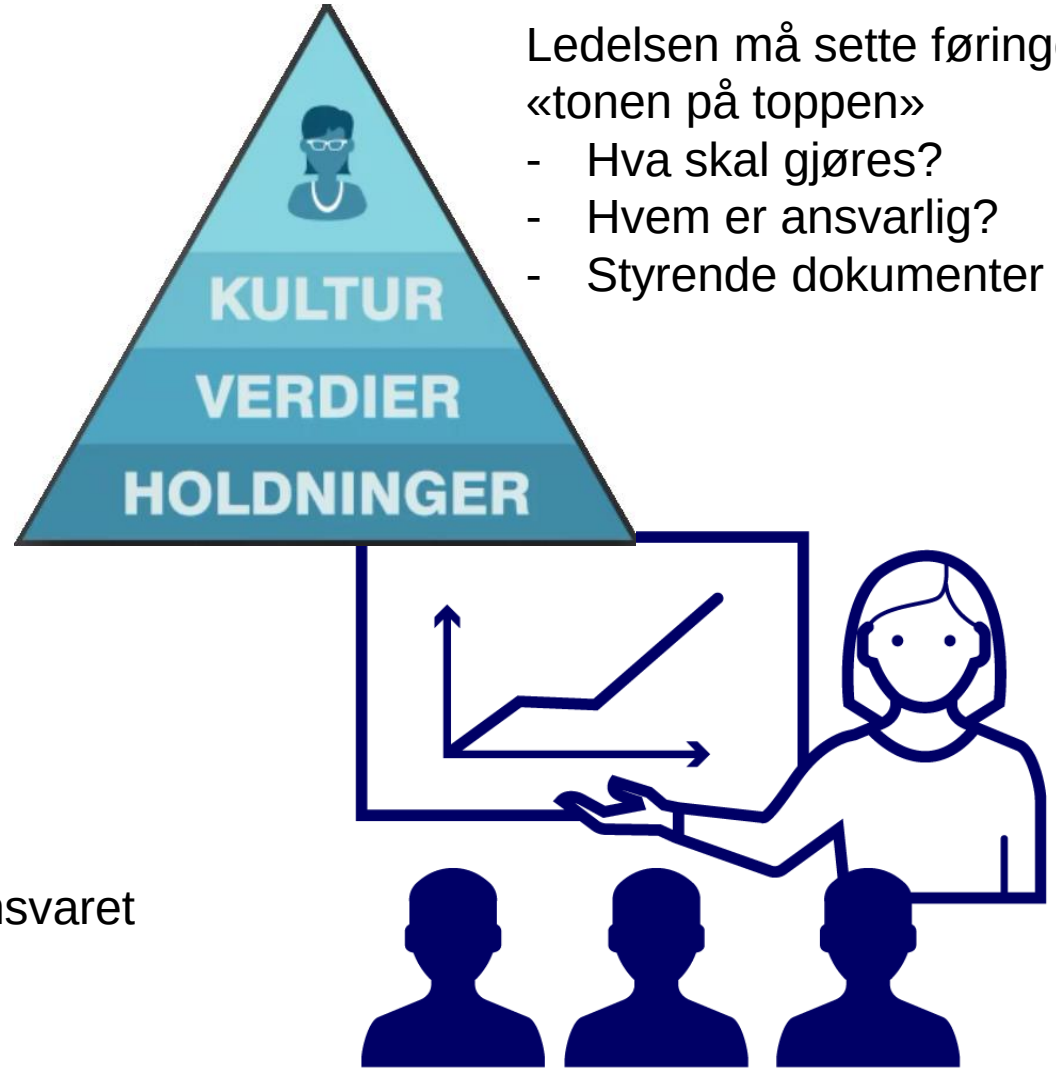

*Virksomhetens leder har det endelige ansvaret for det forebyggende sikkerhetsarbeidet og for at dette arbeidet gir forsvarlig sikkerhet som resultat*

- Virksomhetens leder skal fastsette et styringsdokument for sikkerhet som beskriver:
  - Hvilke verdier skal beskyttes
  - Fordeling av ansvar og myndighet
  - Prinsipper for virksomhetens sikkerhetsarbeid

# Fellestrekk – ledelse og styring



Lederen har det øverste ansvaret

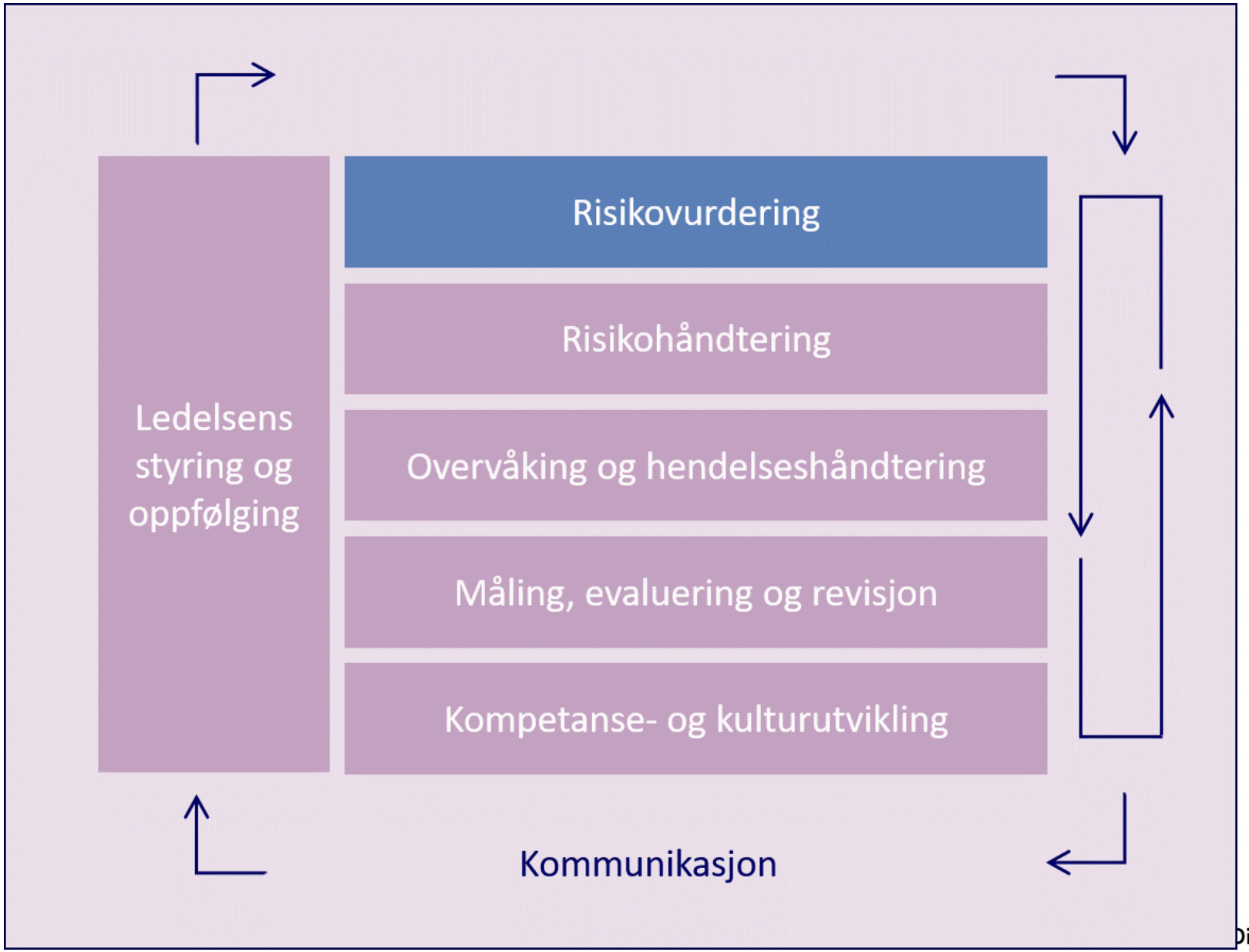



Ledelsen må sette føringene – «tonen på toppen»

- Hva skal gjøres?
- Hvem er ansvarlig?
- Styrende dokumenter

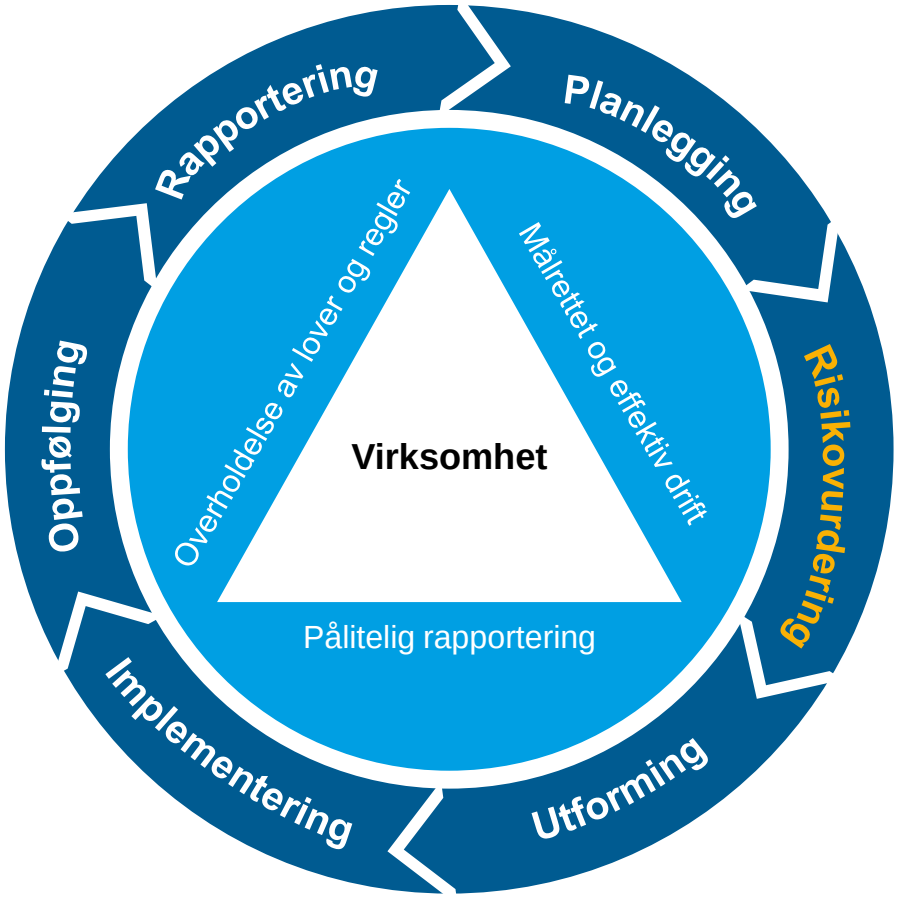
Ansvar for gjennomføring sitter i linjen

# Risikovurdering og risikohåndtering


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

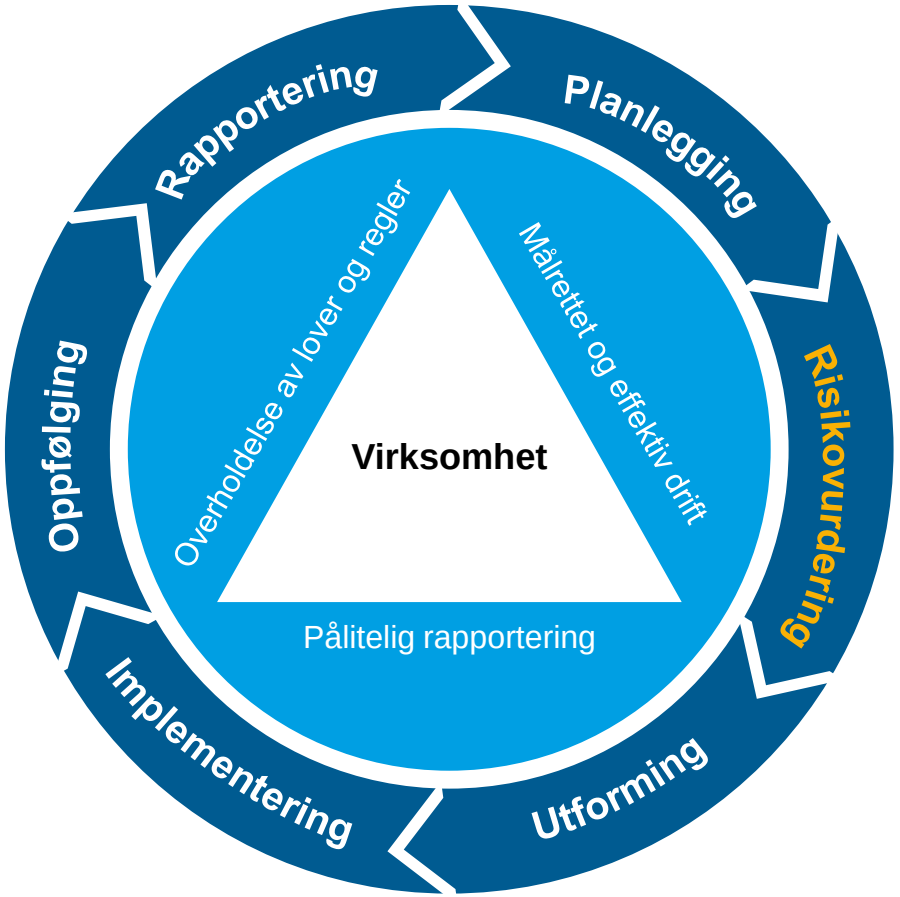
# Risikovurderinger - overordnet

- Ledelsen etabler et grunnlag for risikovurderingen – oversikt over mål og krav
- Ledelsen gjennomfører risikovurderinger knyttet til mål og krav
- Ledelsen vurdere hvilke sentrale aktiviteter/ prosesser, systemer og verdier det er behov for å ha særlig god internkontroll på

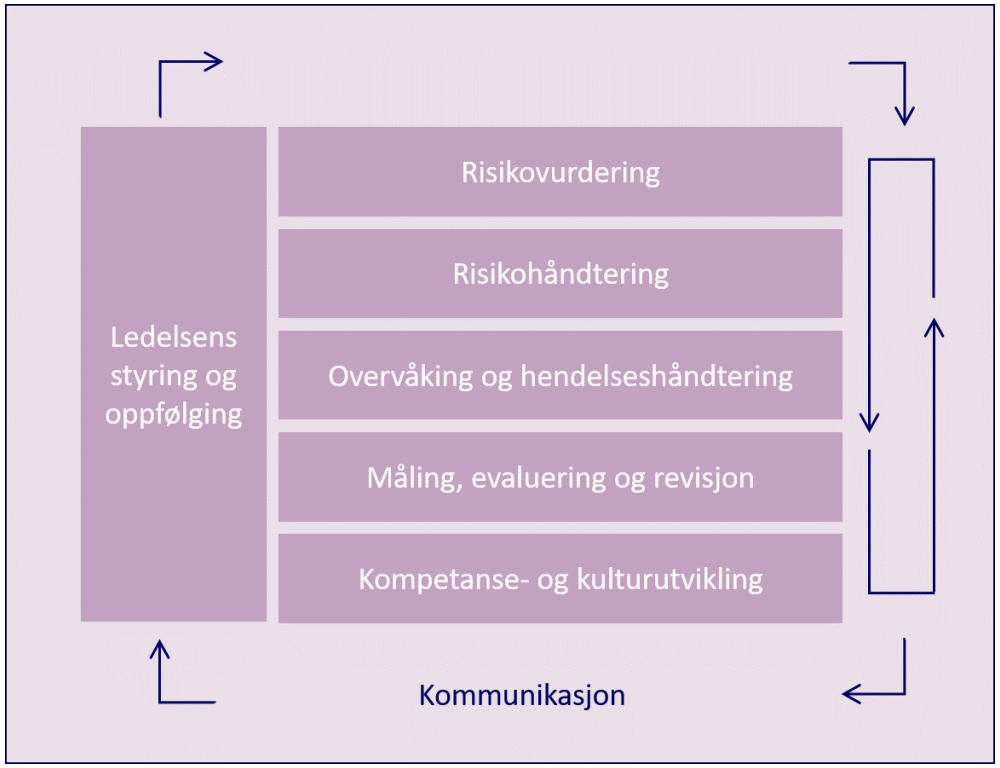


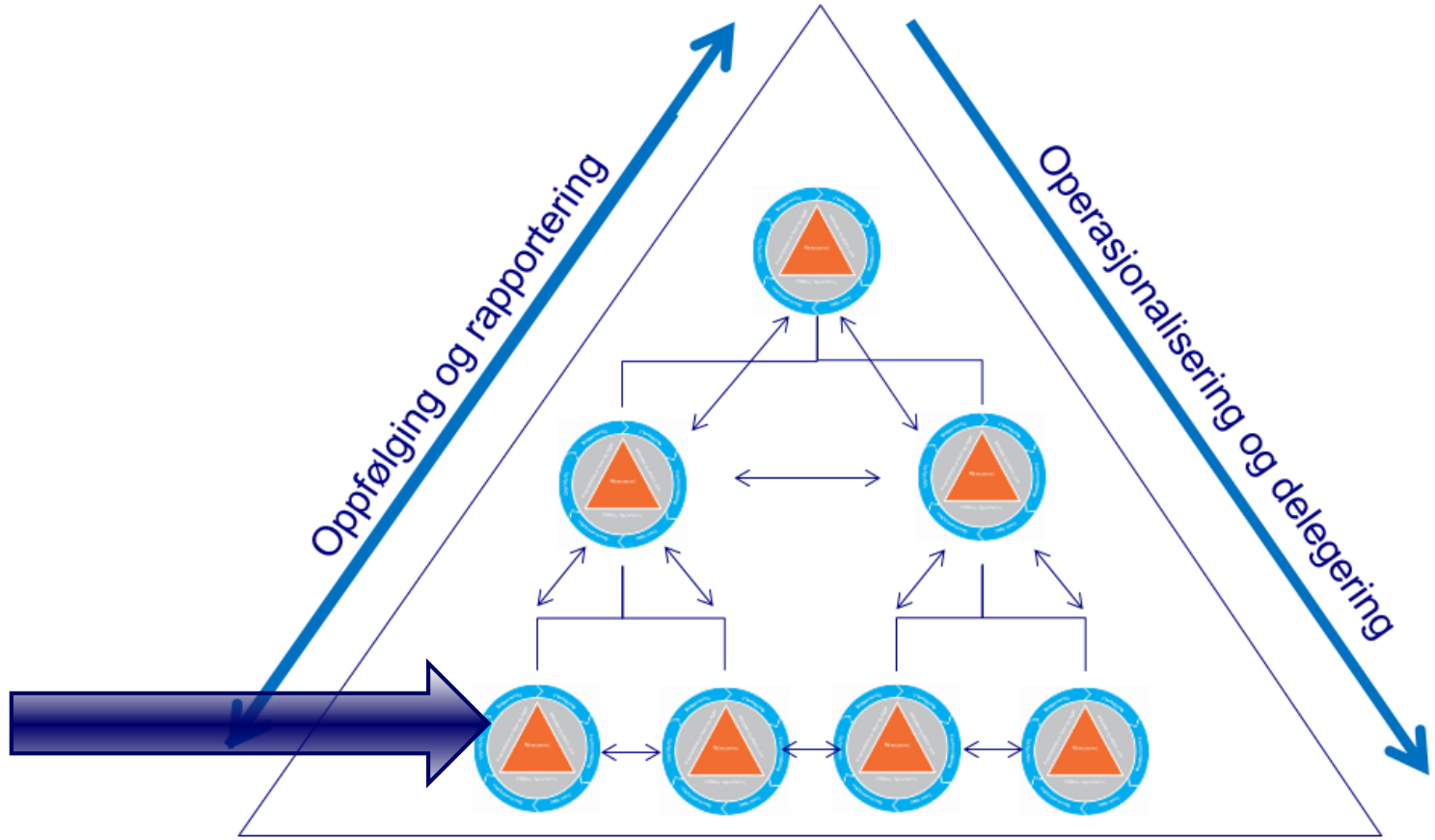
# Risikovurderinger - på lavere organisatoriske nivåer og prosesser

- Ledere på lavere nivåer gjennomfører risikovurderinger og ledelses gjennomgang el. innenfor sitt ansvarsområde
- Dette skjer i henhold til toppledelsen sin risikotoleranse
- Risiko som ikke kan håndteres innenfor eget ansvarsområde rapporteres til nivået over



# Digitaliseringsdirektoratet vs DFØ



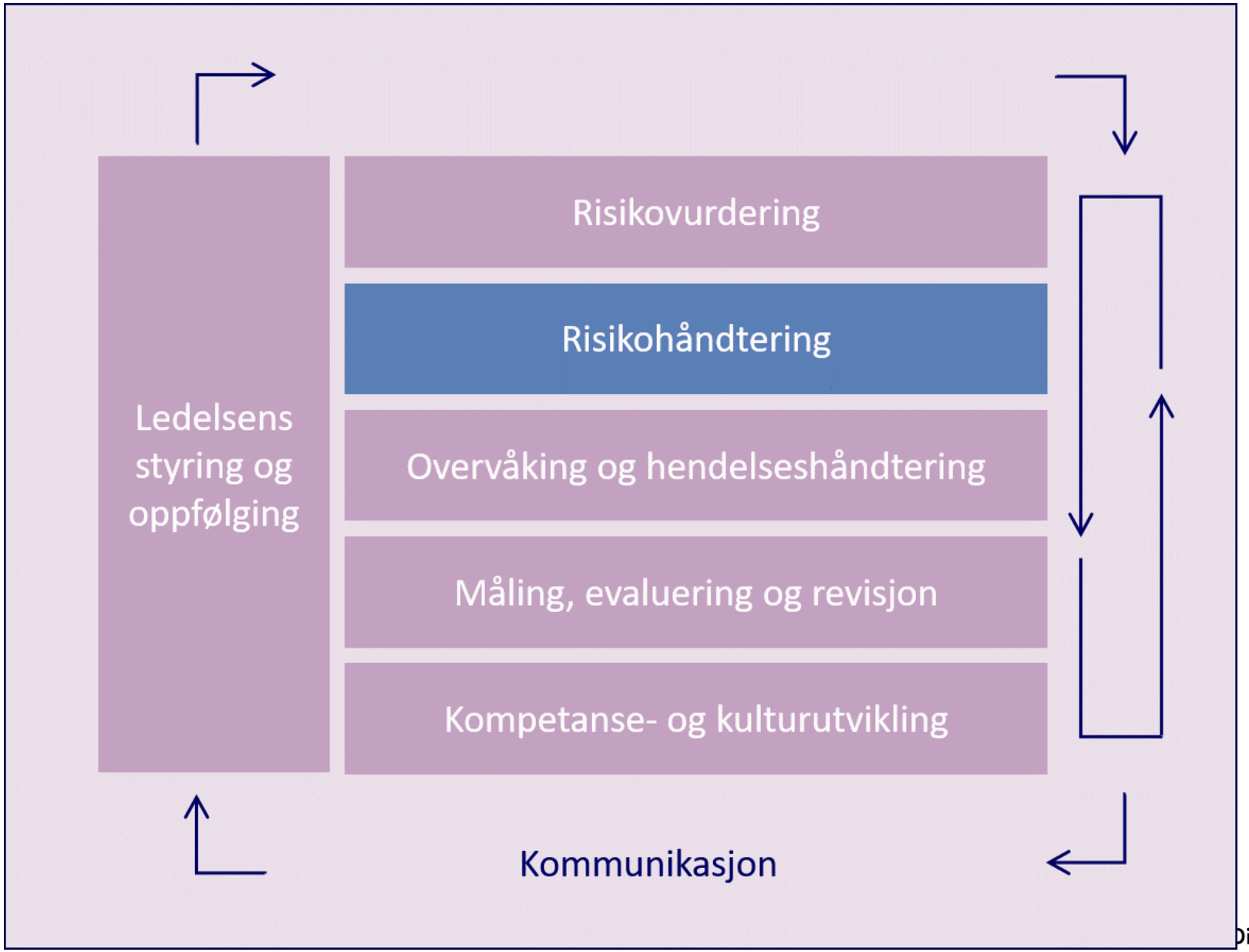




Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

# Risikovurdering

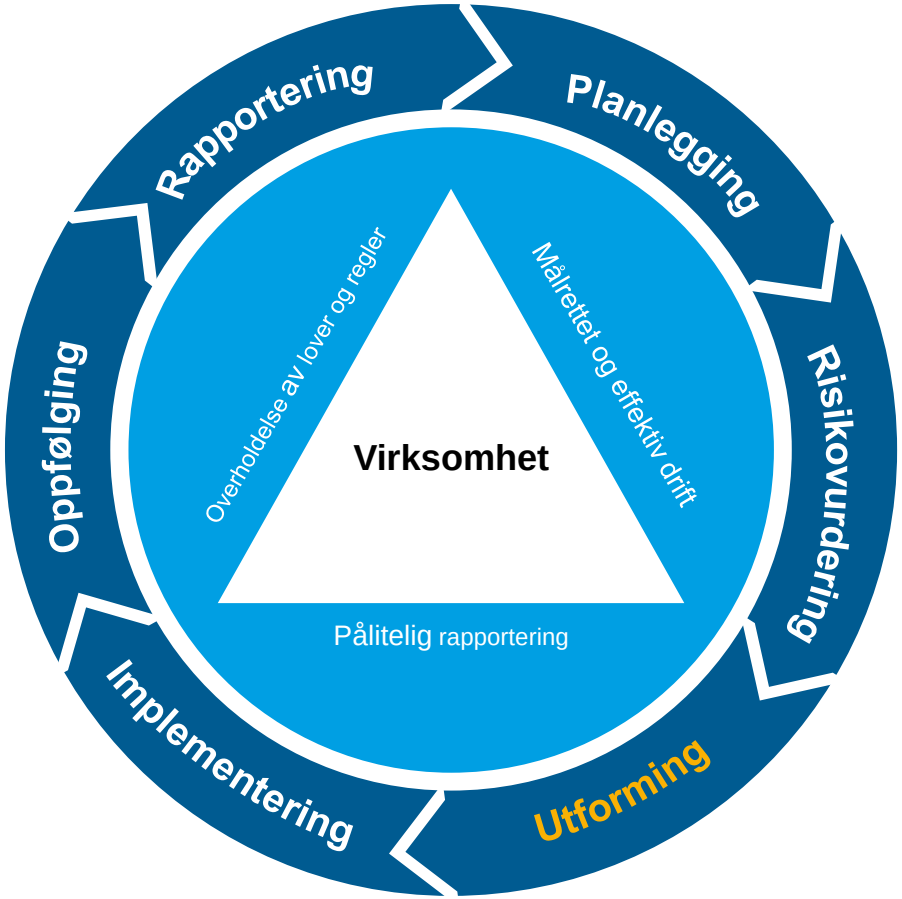
*Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.*

- Når en virksomhet vurderer risiko, skal den ta hensyn til:
  - Eksterne og interne forutsetninger og krav
  - Betydningen skjermingsverdige verdier har for GNF/Nasjonale sikkerhetsinteresser
  - Trusler – inkludert sannsynligheten for at disse kan inntreffe
  - Sårbarheter – inkludert konsekvens ved at sikkerhetstruende virksomhet inntreffer
  - Avhengighet av andre virksomheter


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

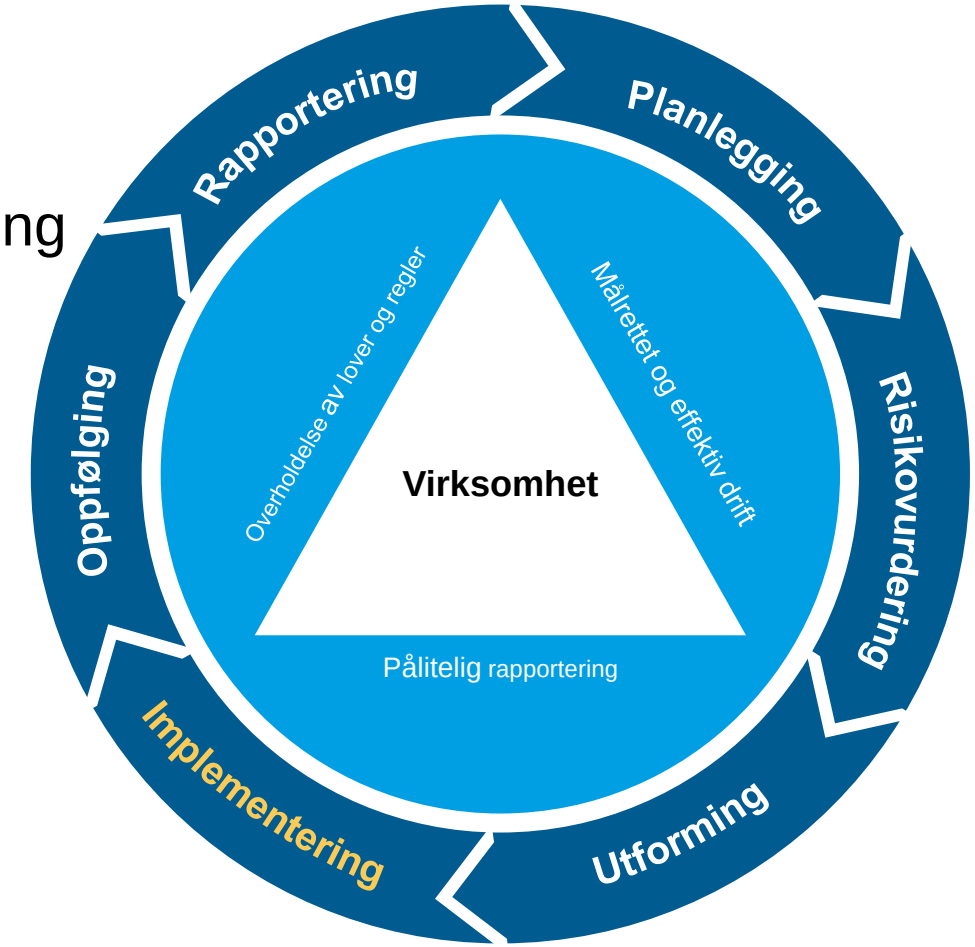
# Tiltak/kontrollaktiviteter blir utformet på ulike organisatoriske nivå for å håndtere uakseptabel risiko

- Identifisere aktuelle tiltak/kontrolltiltak
- Vurdere og prioritere tiltak/kontrolltiltak
- Beslutte tiltak og dokumentere plan for gjennomføring



# Målet med implementering er å sørge for at tiltaket etterleves og får ønsket effekt

- Viktig for å sikre varig endring:
  - Informasjon, kommunikasjon og tilgjengeliggjøring
  - Forankring, holdning og adferd
  - Kompetanse, ferdigheter og kapasitet
  - Verktøy og systemstøtte




Direktoratet for forvaltning og økonomistyring

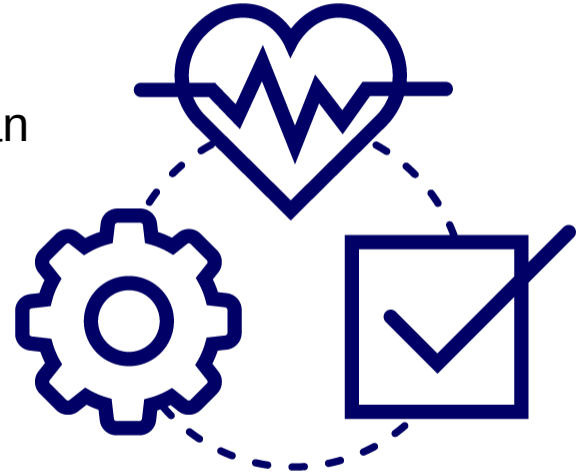
# Risikohåndtering

Virksomheten må vurdere flere forhold i sin håndtering av risiko:

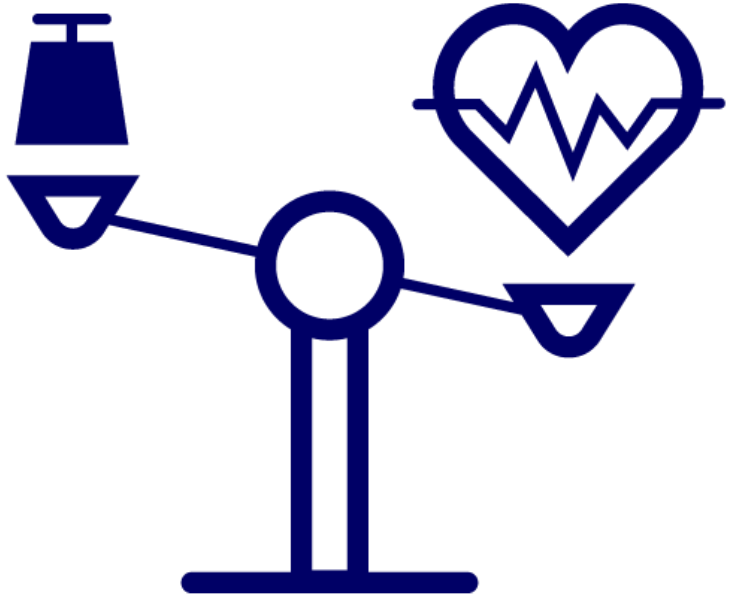
- Er risikoen akseptabel?
  - Hvis ja – forsvarlig sikkerhet!
- Hvilke tiltak kan redusere sårbarheter til akseptabelt nivå?
- Hvilke tiltak er egnet til reduksjon av konsekvenser av sikkerhetstruende virksomhet?
  - Redundans; skadebegrensning; gjenopprettelse?
- Hvordan kan avhengigheter reduseres?
  - Oversikt over avhengigheter sendes til NSM og sektordepartement
- Finnes andre, egnede former for risikoreduksjon?

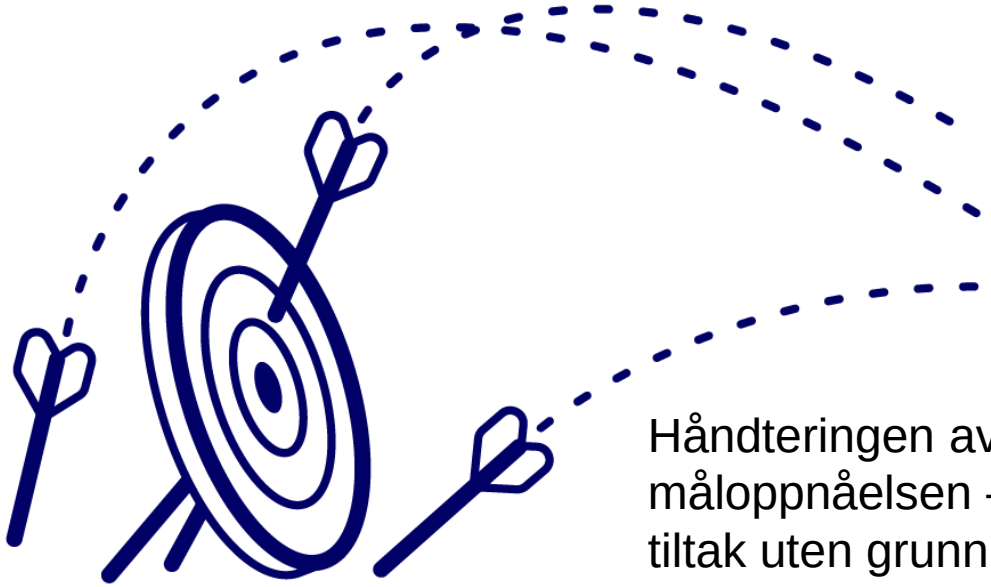
# Fellestrekk – risikovurdering og -håndtering

Ha oversikt – se sammenhengen mellom aktivitetene og arbeidet man gjør, risikoen man står overfor, og implementere tiltak basert på det.



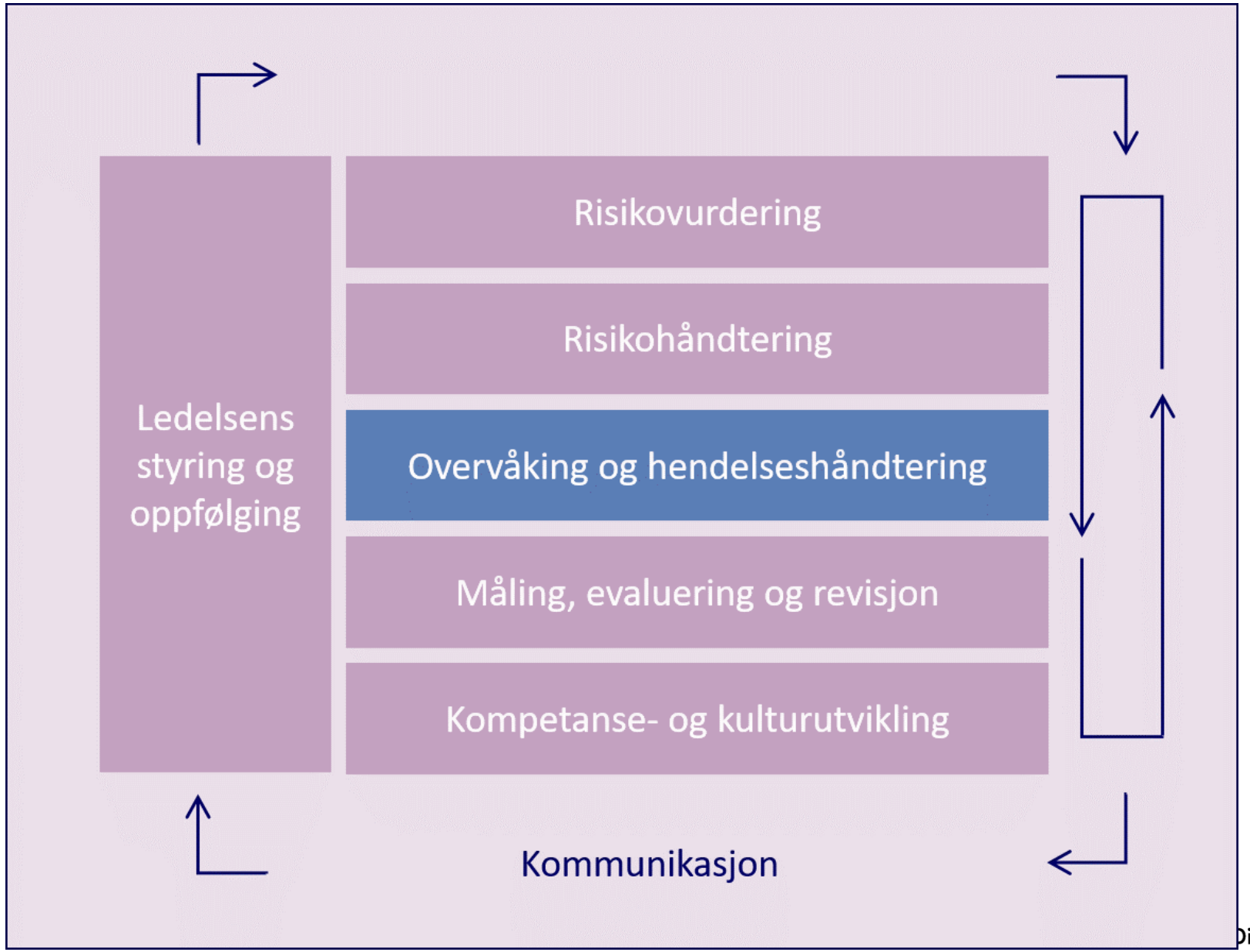
Målet er å håndtere risiko på en tilstrekkelig og forsvarlig måte.

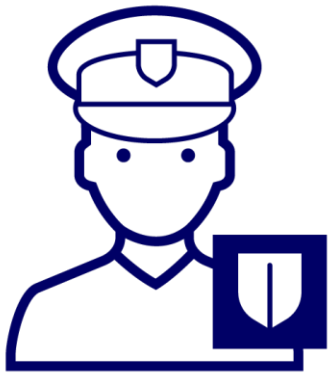


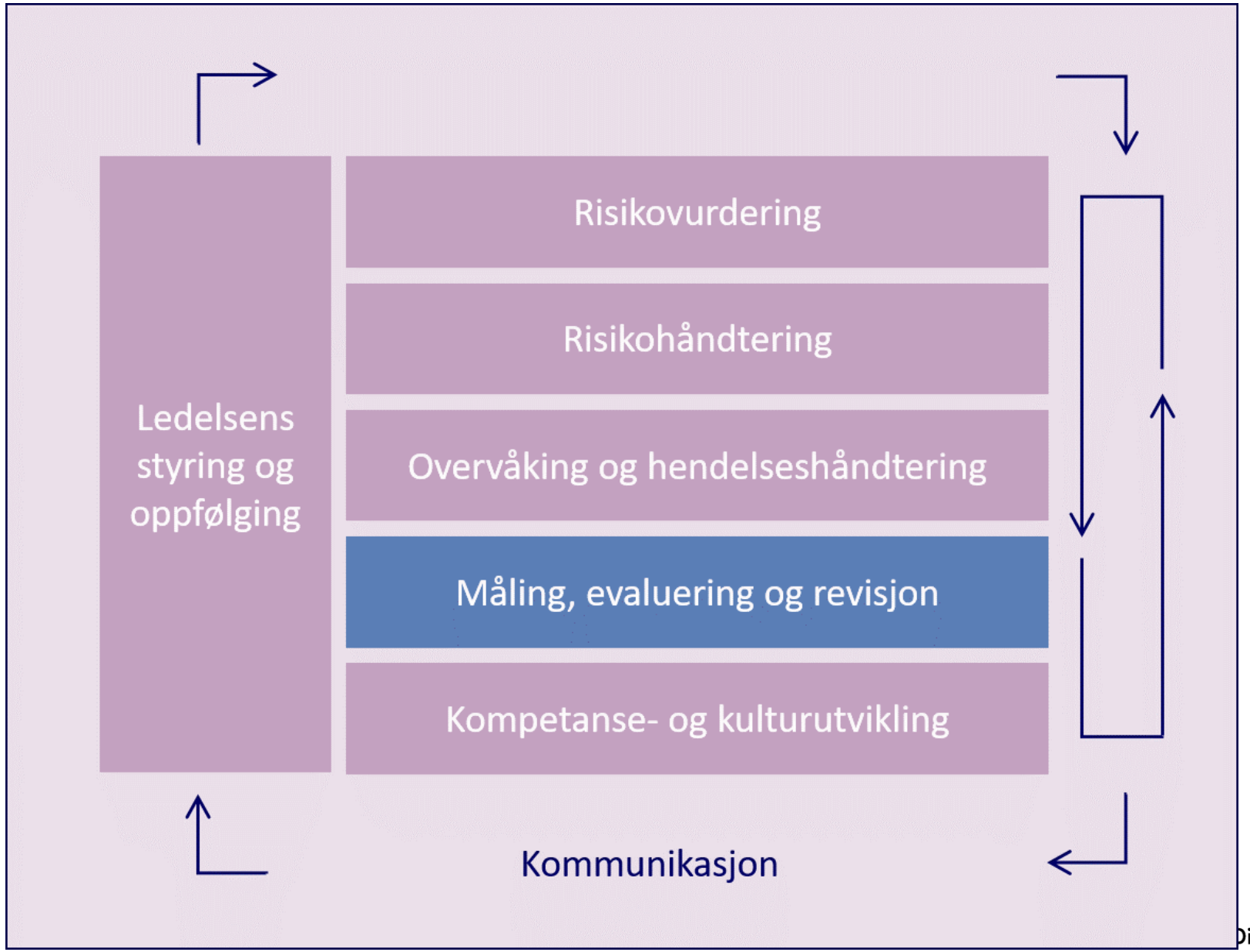


Håndteringen av risiko må underbygge måloppnåelsen – ikke implementere tiltak uten grunn

# Oppfølging og forbedring


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon




Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

# En levende internkontroll forutsetter oppfølging

- Sørg for oppfølging og overvåkning knyttet til det som er viktigst for måloppnåelsen

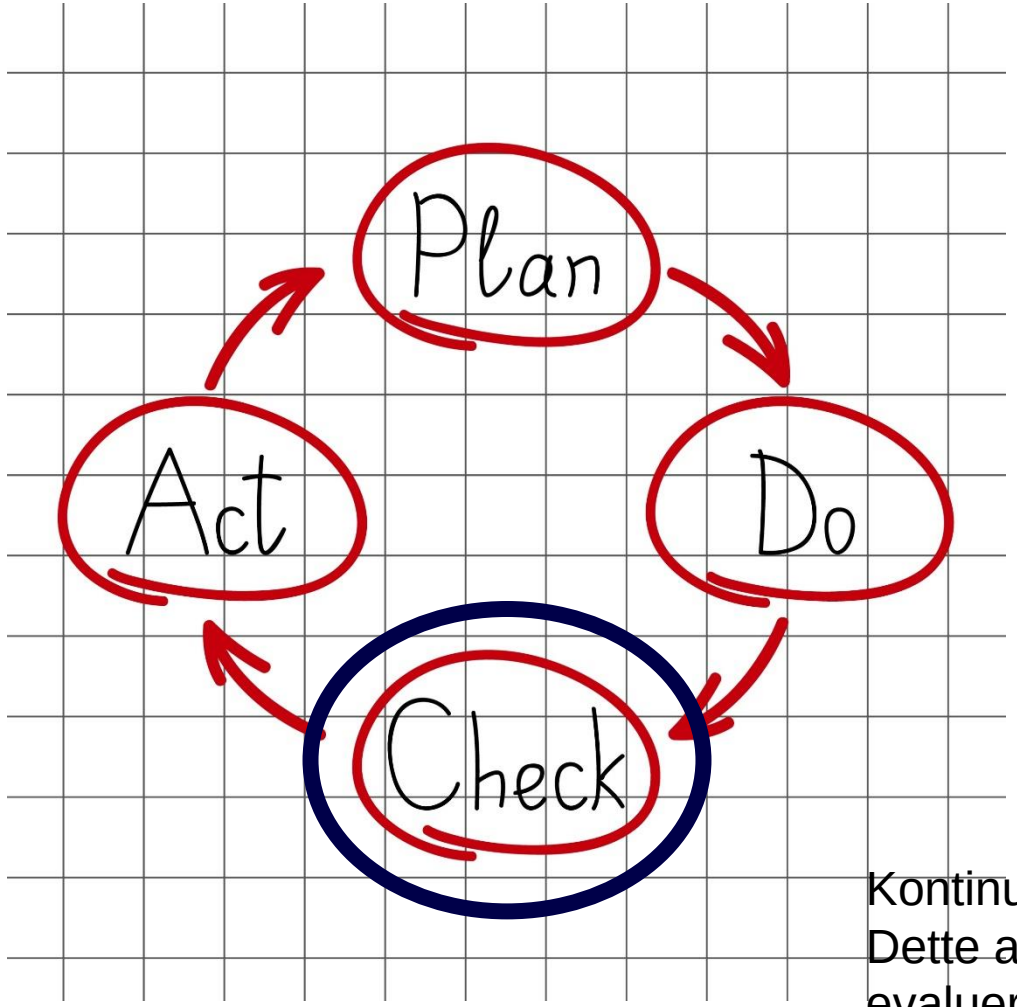
- Løpende eller frittstående oppfølging av internkontrollen for å vurdere…
  - om den gir ønsket effekt, som vil si at tiltak/kontrollaktiviteter fungerer som forventet
  - om tiltak/kontrollaktiviteter blir etterlevd, det vil si om vi gjør det ledelsen har bestemt

# Sikkerhetsoppfølging

Forebyggende sikkerhetsarbeid gjennomføres i en kontinuerlig forbedringsprosess

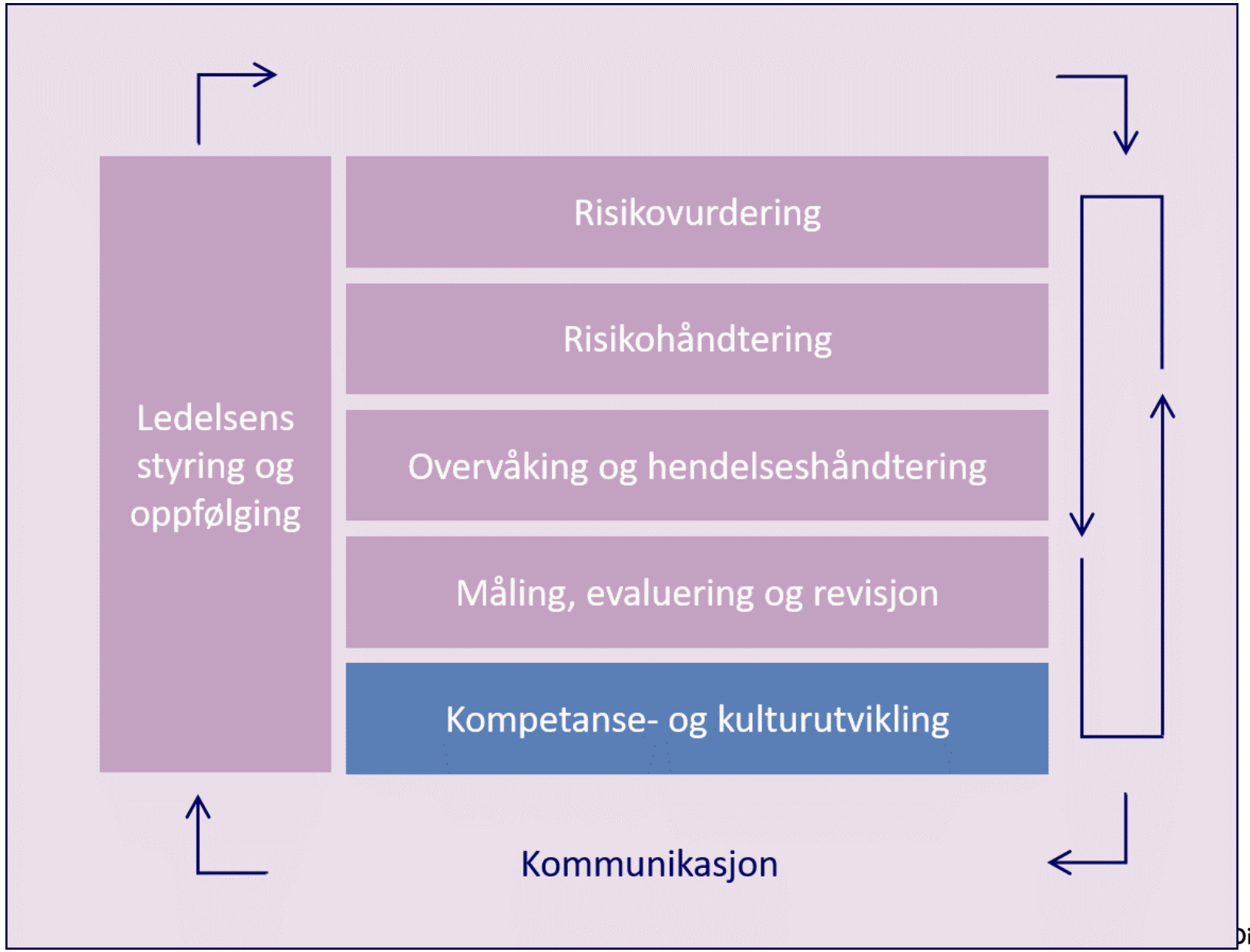
- Kontroll av arbeidsutførelse
- Håndtering av sikkerhetstruende hendelser
  - Varsling, strakstiltak, begrensing, gjenoppretting
- Evaluering og øvelser
  - Min. årlig kontroll av styringssystemet for sikkerhet
  - Øvelser for å kontrollere effekten av sikkerhetstiltak i normalsituasjon og ved økt trusselnivå
- Ledelsens gjennomgang av det forebyggende sikkerhetsarbeidet

# Fellestrekk – oppfølging og forbedring




Kontinuerlig forbedring er en forutsetning
Dette avhenger av oppfølging og evaluering, og at man lærer av hendelser

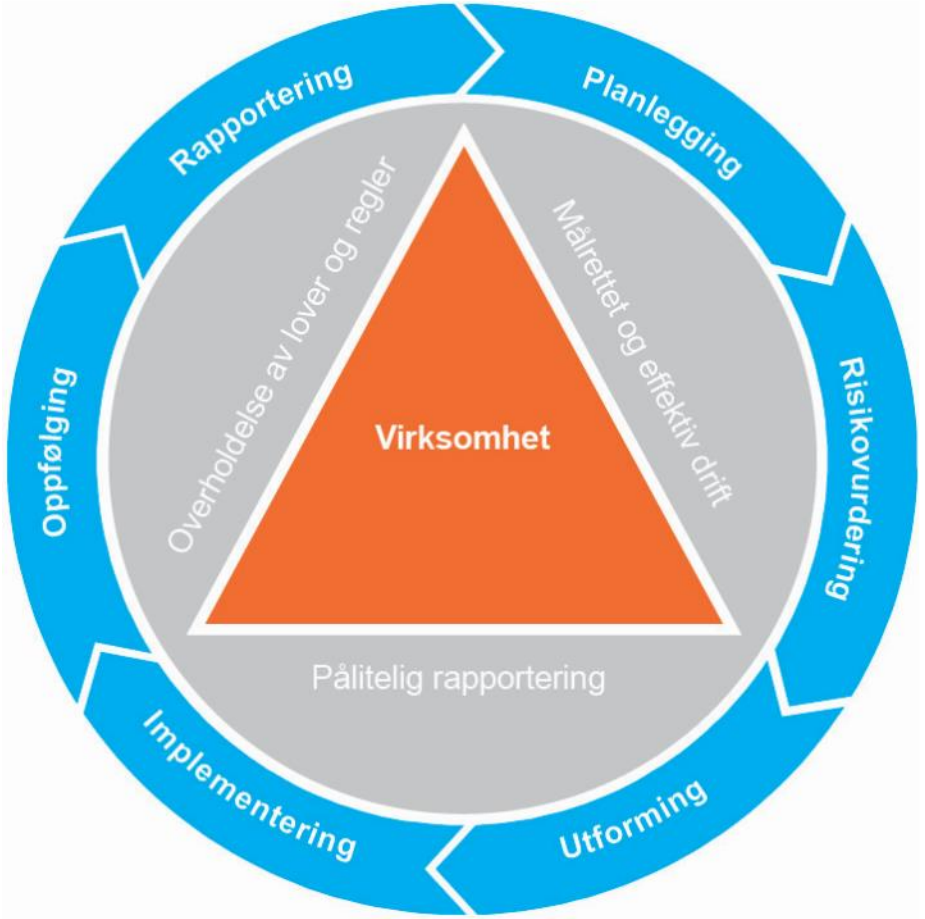
# Kompetanse og organisering


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon


A

# Fundamentet for god internkontroll

- Styrings- og kontrollmiljø:
  - «Tonen på toppen»
  - Kompetanse
  - Integritet og etiske verdier
  - Ledelsesfilosofi
  - Organisasjonsstruktur
  - Fordeling av roller og ansvar
  - Personalpolitikk



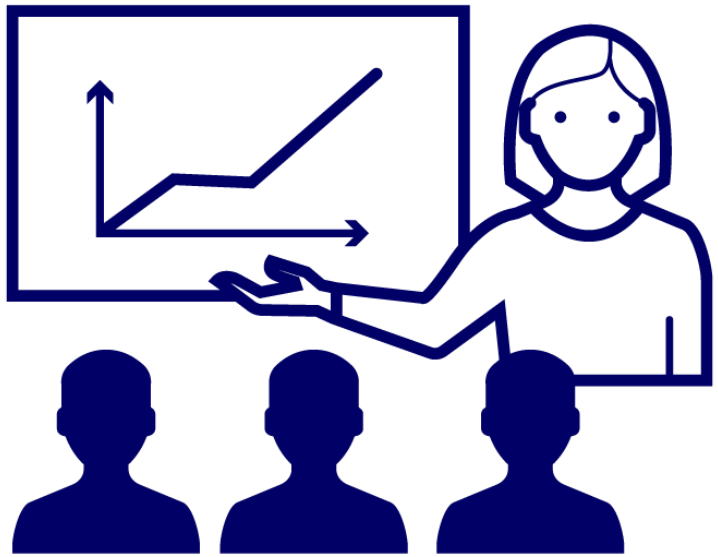
# Sikkerhetsorganisering

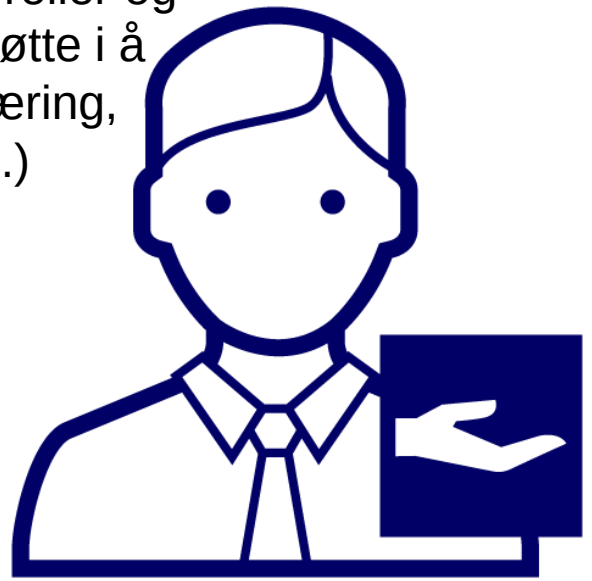
Sikkerhetsorganisering omfatter fordeling av ansvar og myndighet for utførelse av sikkerhetsoppgaver samt klargjøring av forutsetninger og plikter for den enkelte

- Sikkerhetsforståelse
  - God sikkerhetskultur
  - *«Verdivurderer vi rett?»*
- *Kompetanse*
  - *Helhetlig tilnærming til fag og sikkerhetsarbeid*
  - *«Har de ansatte tilstrekkelig kompetanse til å behandle skjermingsverdig informasjon?»*
- Rollefordeling
  - Beslutning, utførelse og oppfølging
  - *«Har virksomheten de roller som kreves for å kunne verdivurdere og behandle skjermingsverdig informasjon?»*

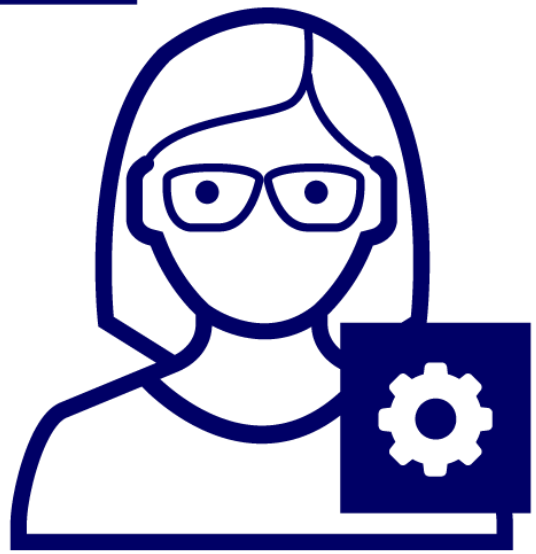
# Fellestrekk – kompetanse / organisering

Det må være definert klare roller og ansvar, og ansatte må få støtte i å utføre sine oppgaver (opplæring, verktøy, støtteressurser etc.)

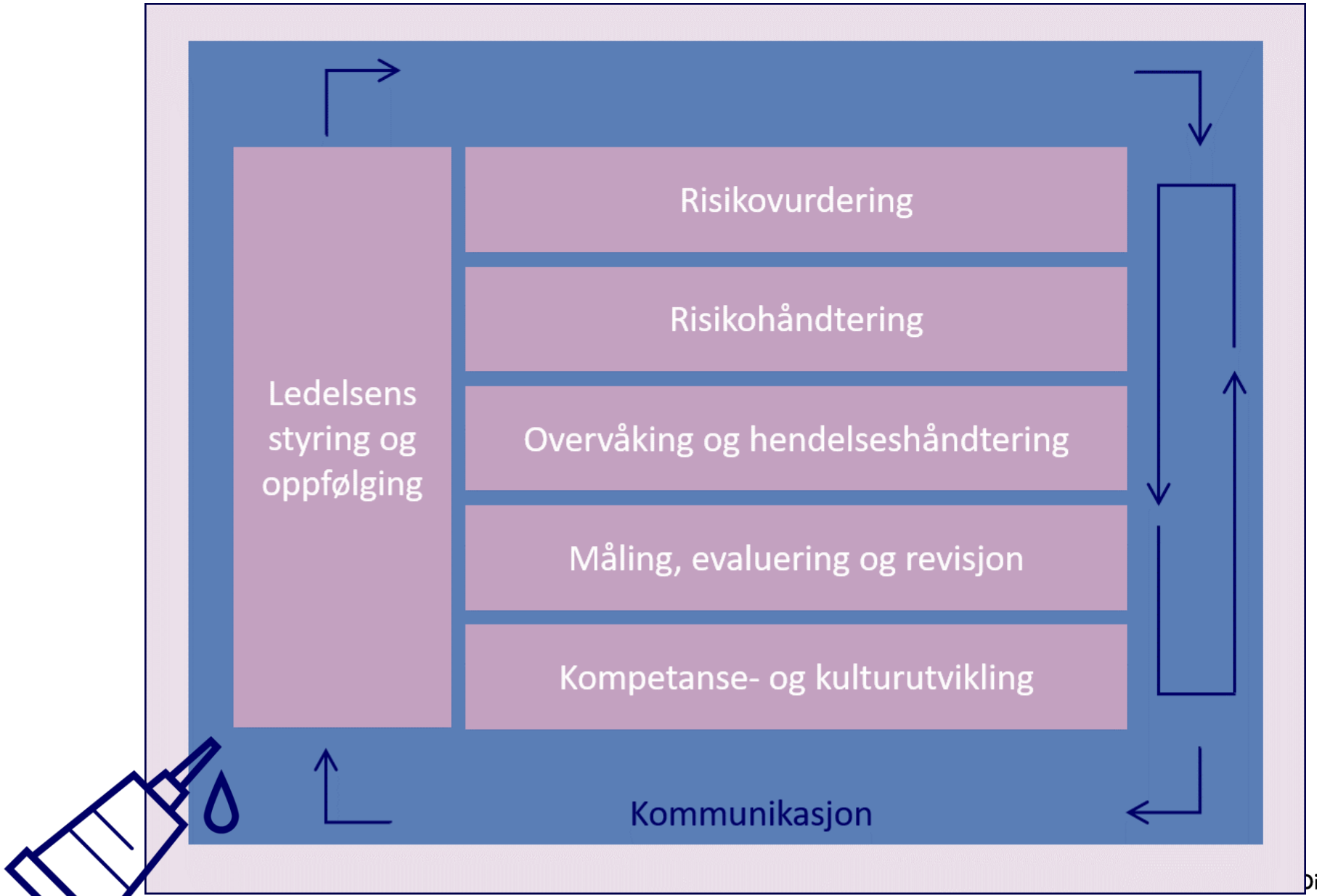




Ansatte som utøver oppgaver må ha tilstrekkelig kompetanse til det.

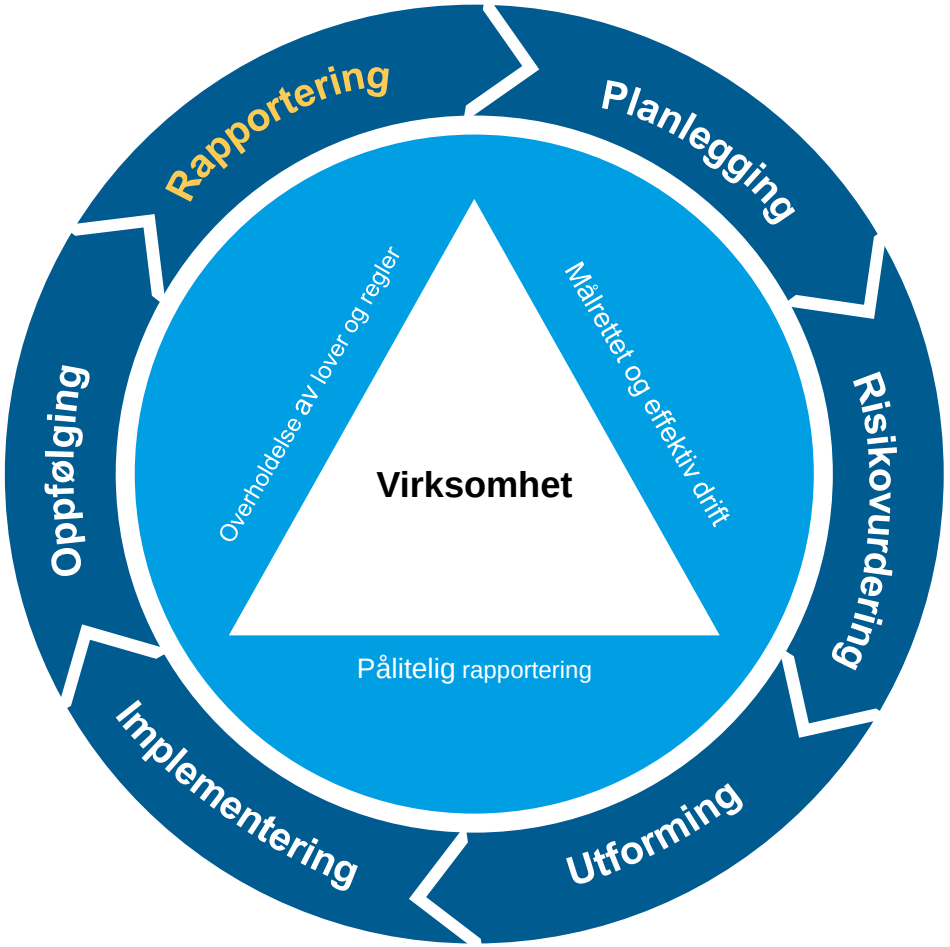


# Dokumentasjon og kommunikasjon


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

# Resultatet av oppfølgingen må rapporteres til rett nivå til rett tid

- Rapportering knyttet til internkontrollen bør integreres med øvrig rapportering
- Rapporteringen gir grunnlag for vurdering av internkontrollsystemet og vurdering av om kritiske risikoer er tilstrekkelig håndtert, ref. kap. 4 Styring og kontroll i årsrapporten
- Informasjonen om status på internkontrollen i rapporteringen bør benyttes inn i styringen, dvs. planlegging og risikovurdering




**Ikke *mer* rapportering, men *bedre* og kun *nødvendig* rapportering**

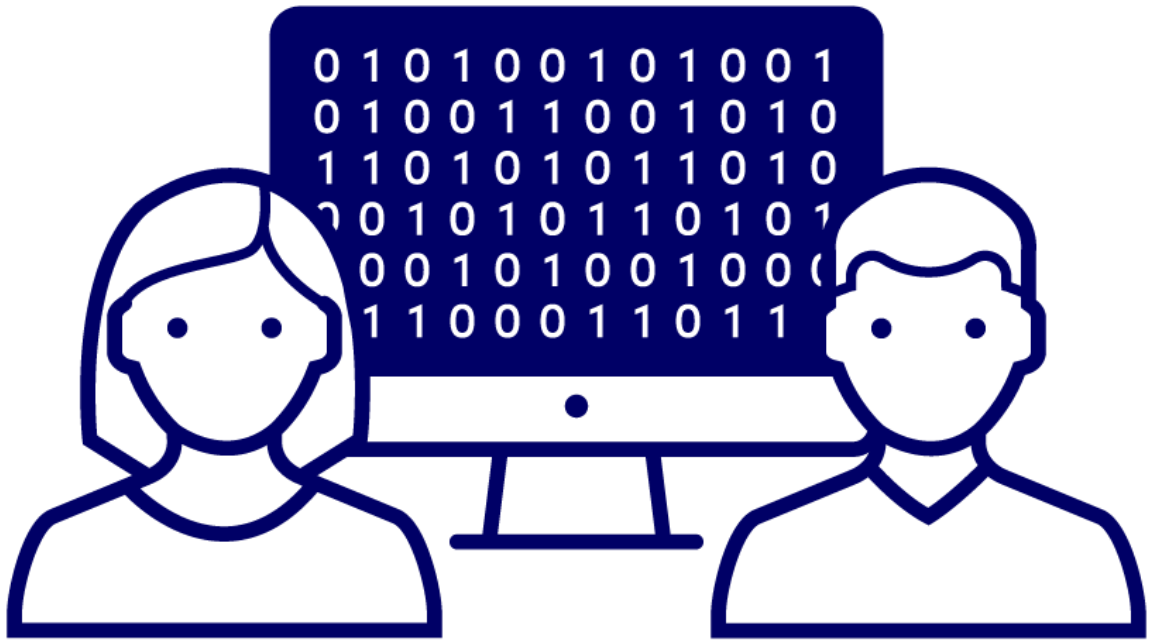
# Sikkerhetsdokumentasjon

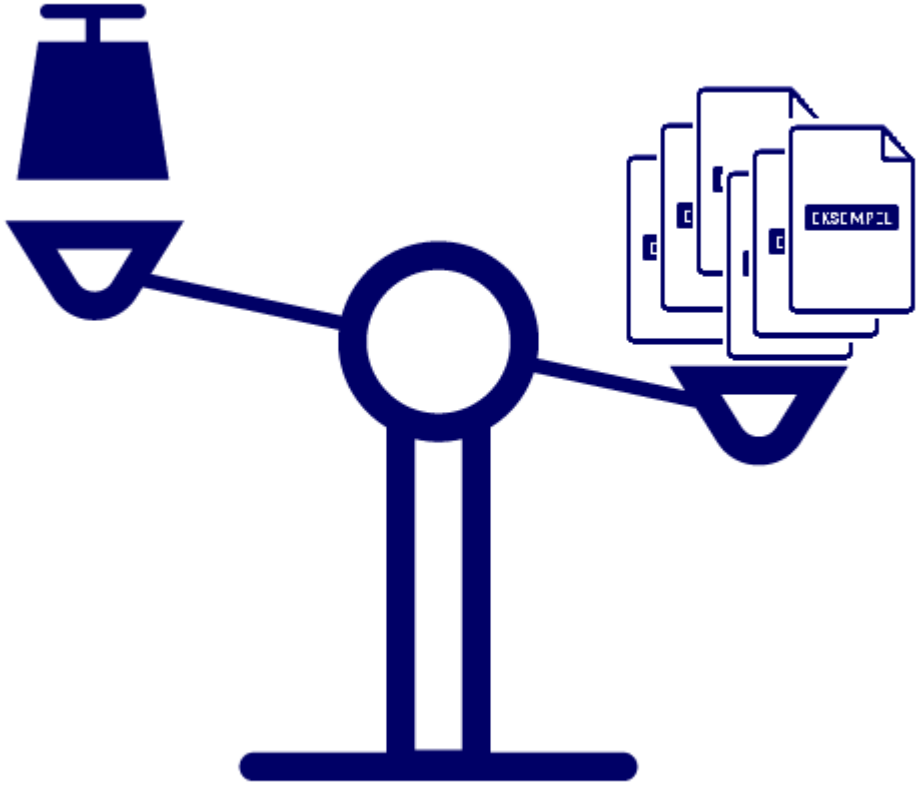
Sikkerhetsstyringssystemet må være tilstrekkelig dokumentert, og hvordan sikkerhetsarbeidet skal utføres skal fremkomme i dokumentasjonen

- Sikkerhetsstyringssystemet dokumenteres i det omfang det er nødvendig for å sikre at aktiviteter utføres sikkert og som besluttet
  - Styrende dokumenter – policy, retningslinjer
  - Utførende dokumenter – instrukser, rutiner
  - Kontrollerende dokumenter – referater, logger, vurderinger, revisjoner

# Fellestrekk – dokumentasjon

Dokumentasjon er en forutsetning for at styringen skal fungere, men den må avveies slik at det er tilstrekkelig, men ikke blir unødvendig mye arbeid.





# Felles utgangspunkt – få oversikt over arbeidsoppgaver og informasjonstyper

# Identifisere arbeidsoppgaver og informasjonstyper

| Om arbeidsoppgaven og formålet | | | |
|---|---|---|---|
| Navn på arbeidsoppgave: | Saksbehandling | Dato: | |
| Formål med arbeidsoppgaven: | | | |
| Kort beskrivelse av arbeidsoppgaven: | | | |

| Om informasjonsbehandling i oppgaven | | | | | | | |
|---|---|---|---|---|---|---|---|
| Informasjonstyper | Paragraf for potensiell taushetsplikt / unntak fra offentlighet | Spesielt obs mht. info.sikkerhet | | | Person-opplysninger | | Skjermings-verdig (sl) |
| | | K | I | T | Ja/? | Særlig kategori? | Ja/? |
| Avsender (?) | Fvl §13.1 | K | | | J | | |
| Kontaktinfo | Fvl §13.1 ? | ? | | | J | | |
| Mottatte saksdokumenter | Fvl §13.1 | K | | ? | J | | |
| Interne vurderinger | Fvl §13.1 | K | I | ? | J | | |
| Beslutning | Fvl §13.1 | K | I | | J | | |
| Klage | Fvl §13.1 | K | | ? | J | | |
| Klagevurdering | Fvl §13.1 | K | I | ? | J | | |
| Klagebeslutning | Fvl §13.1 | K | I | | J | | |

| Ytterligere informasjon |
|---|
| Navn på IKT-system som benyttes til behandling av informasjon: |
| Sak-arkiv |
| Relevant regelverk for gjennomføring av arbeidsoppgaven: |
| fvl, offl, arkivlov |
| Regelverk med krav til informasjonssikkerhet: |
| pvf art 32-34 |
| Merknader: |
| |

# Identifisere arbeidsoppgaver og informasjonstyper

| Etterlevelse av personvernregelverket |
| --- |
| Behandlingsgrunnlag (pvf art 6 og ev. art 9): |
| Pvf art 6 nr 1 bokstav c (arkivlov og relevant regelverk) |
| Angi kategorier av registrerte (for eksempel pasienter, ansatte, kunder, søkere, elever osv.): |
| |
| Angi kategorier av mottakere som opplysningene deles med (for eksempel offentlige myndigheter, allmenheten, parter i saker, etc) |
| Parter/allmennheten (innsynskrav, ev. sladdet) |
| Høy personvernrisiko? Er det behov for en nærmere vurdering av personvernkonsekvenser? |
| |
| Utleveres eller behandles opplysningene utenfor EØS? |
| |
| **Etterlevelse av sikkerhetsloven** |
| |
| **Deling av data** |
| Er det noe av denne informasjonen som andre kan ha nytte av? Hvordan bør det tilrettelegges for deling (f.eks. synliggjøring i datakatalog, publiseres som åpne data?) |
| |

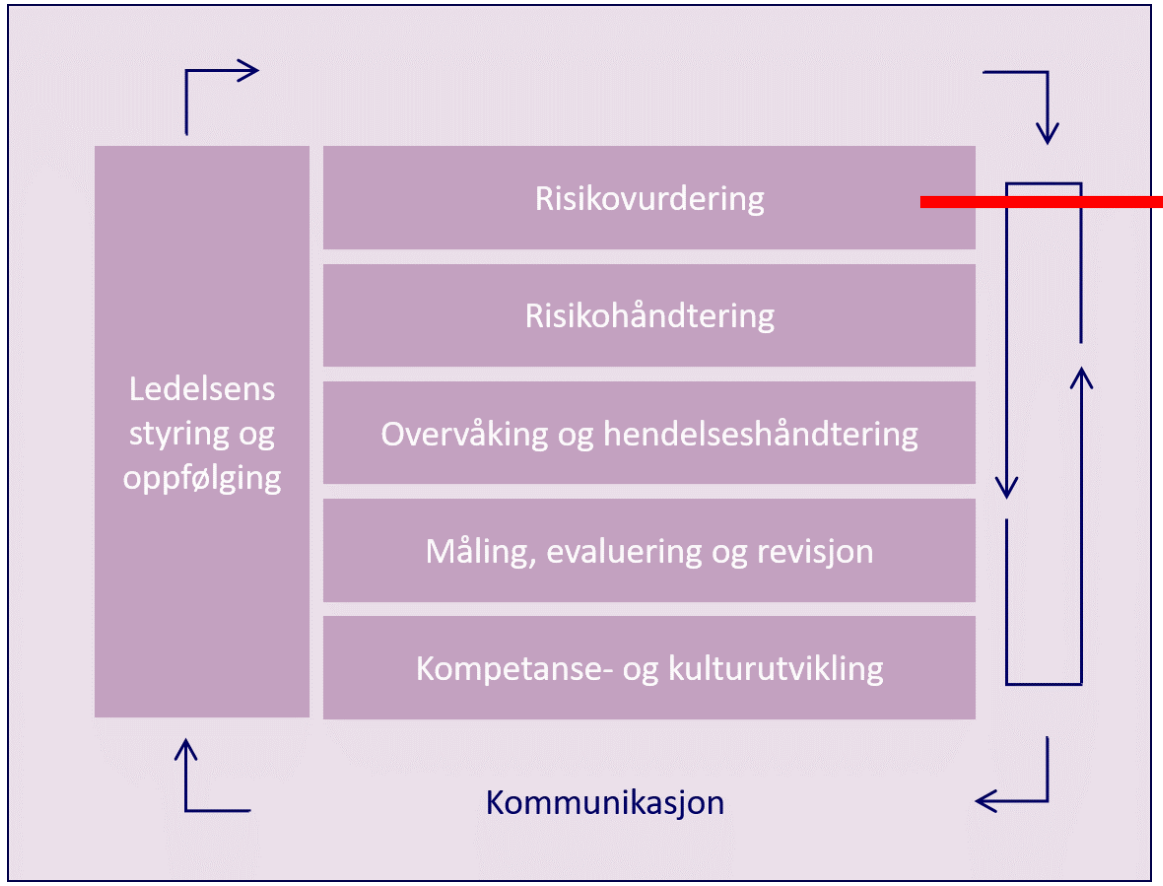
# Få oversikt og prioritere før risikovurderinger

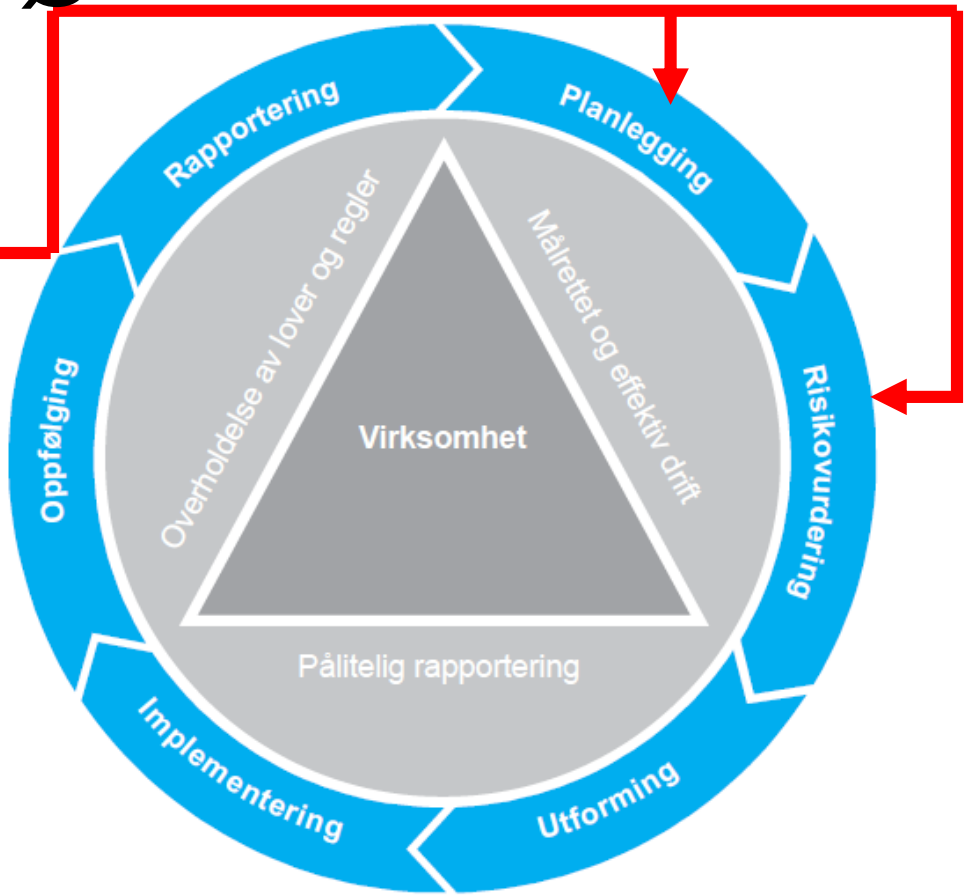
- Positive sideeffekter:
  - Kan gi nyttige refleksjoner og innspill til
    - bedre etterlevelse av personvernregelverket utover informasjonssikkerhet
    - identifisere behov for videre vurderinger etter sikkerhetsloven
    - muligheter for datadeling iht. krav i Digitaliseringsrundskrivet
    - prosess for identifisering og sikring av dokumentasjon
    - prosessforbedringer i den enkelte enhet
    - samordning av prosesser på tvers i virksomheten

- Unngå å gjøre samme jobben flere ganger!

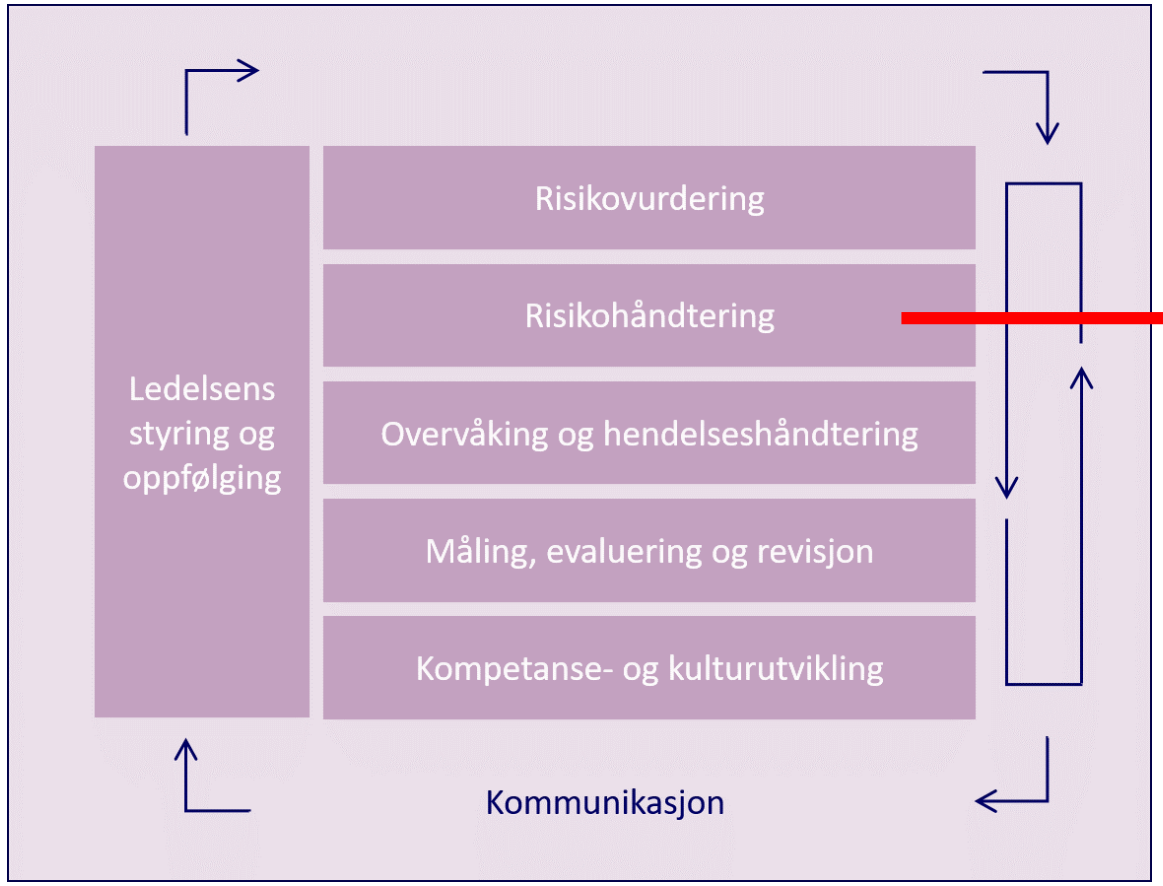
# Oppsummering

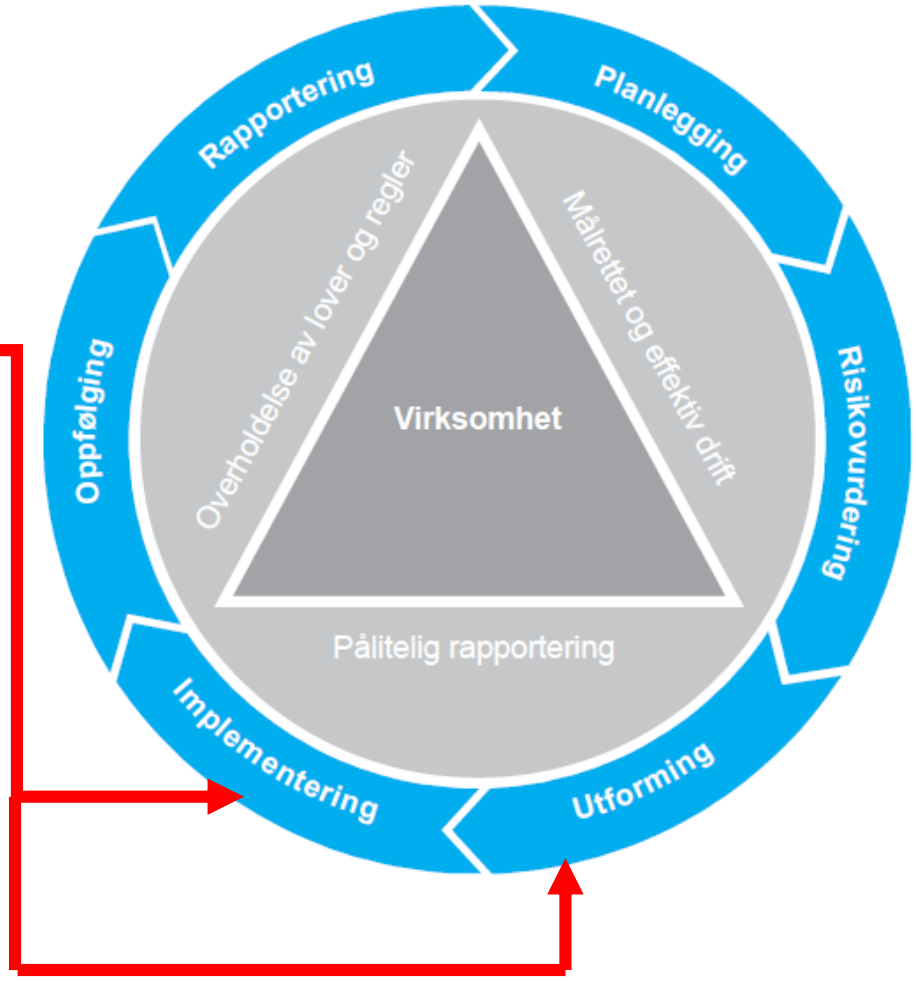
# Digitaliseringsdirektoratet vs DFØ



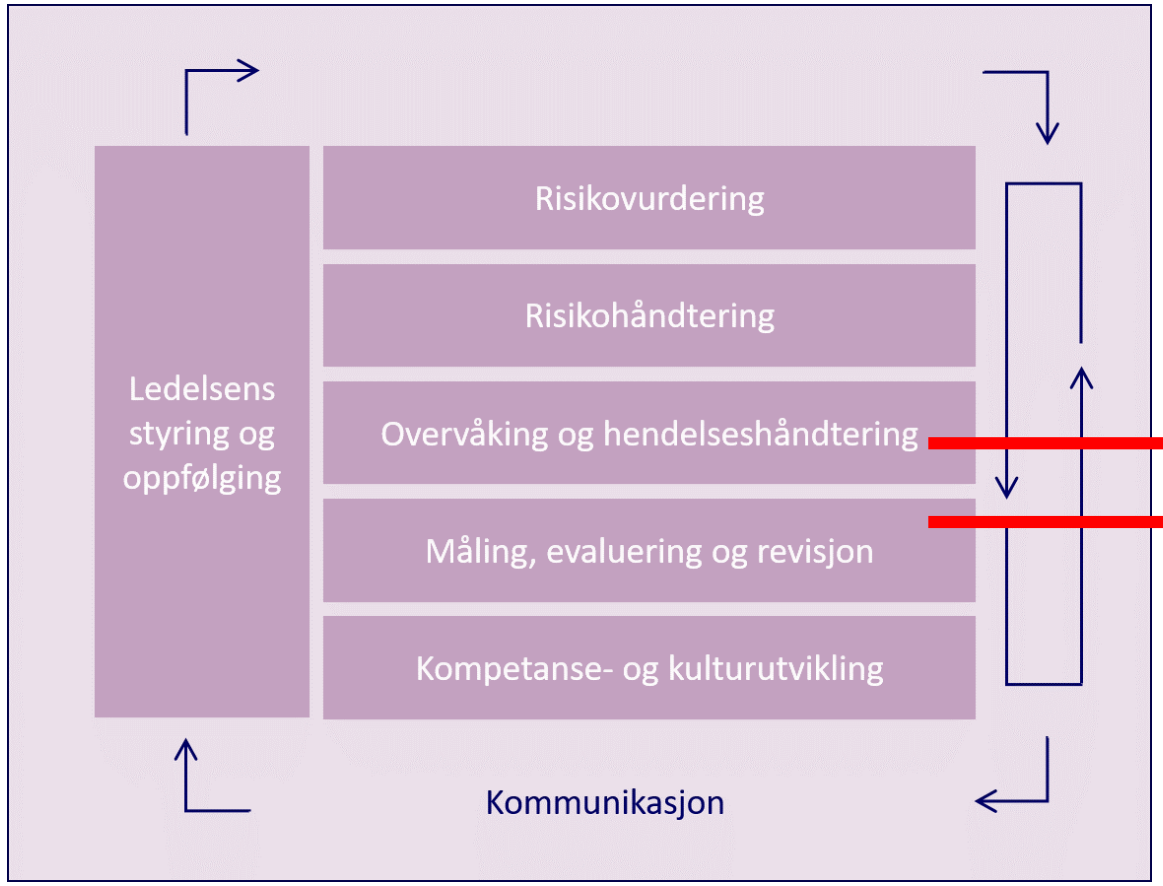



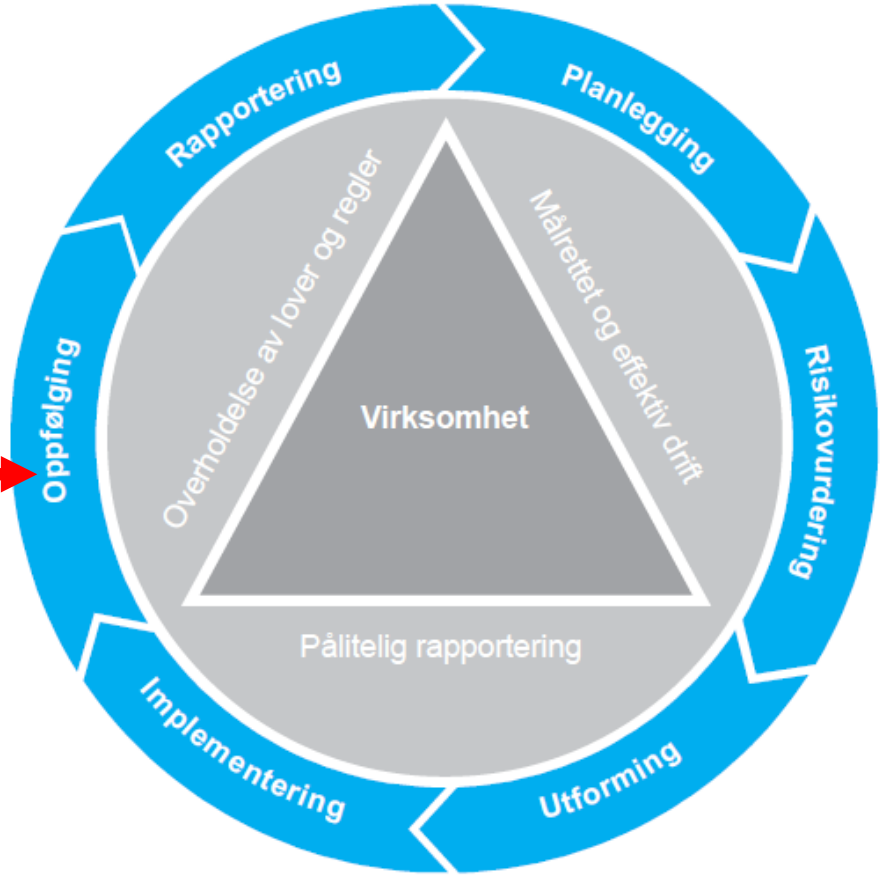
# Digitaliseringsdirektoratet vs DFØ



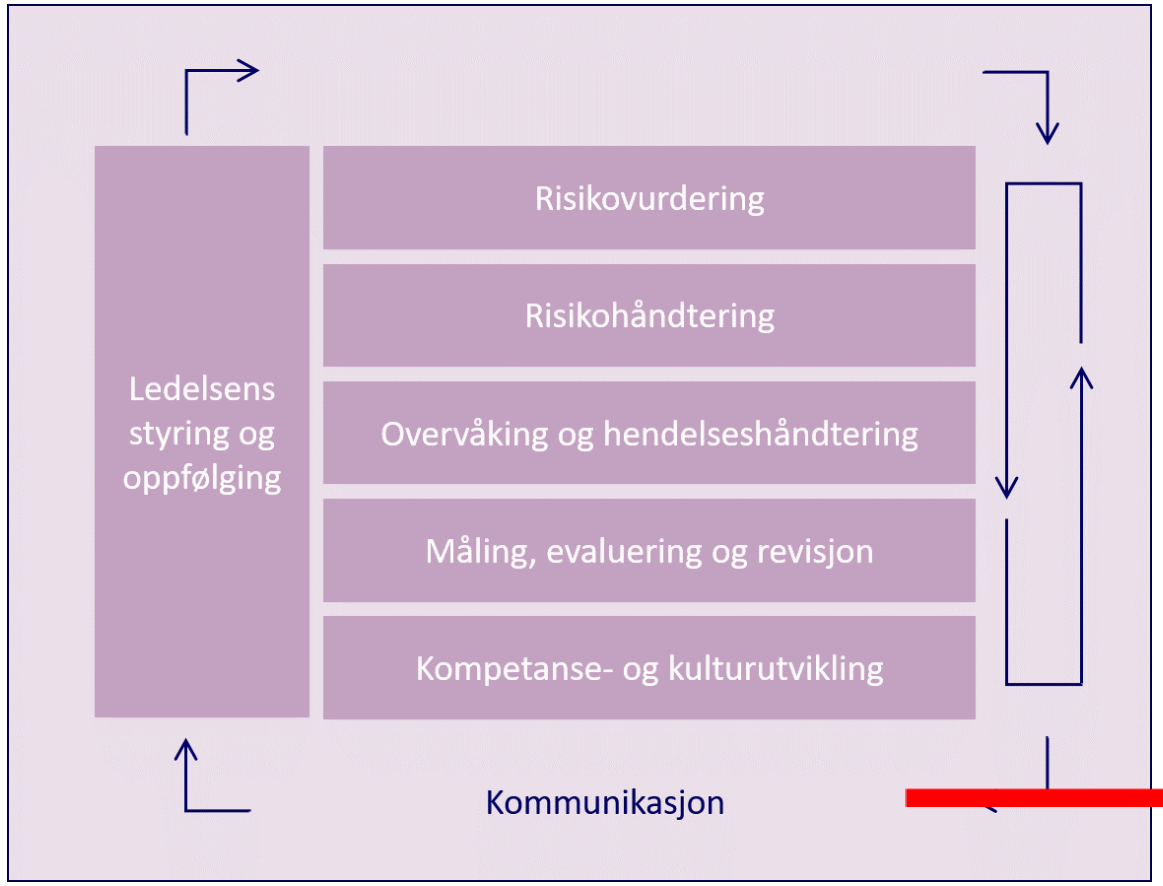



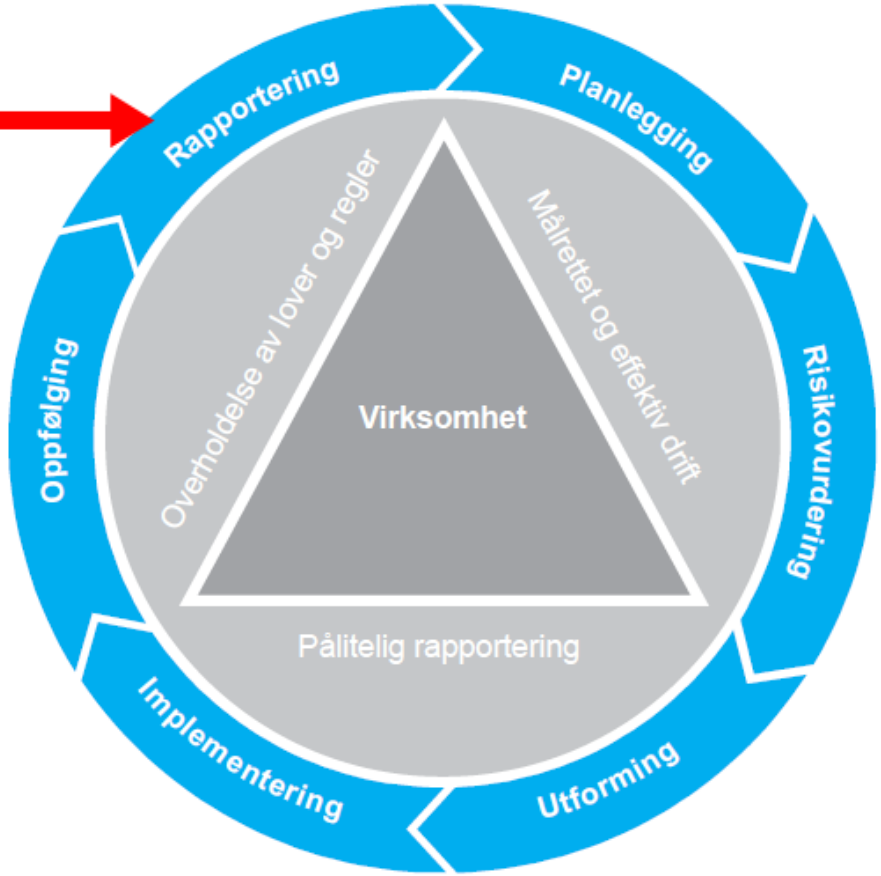
# Digitaliseringsdirektoratet vs DFØ

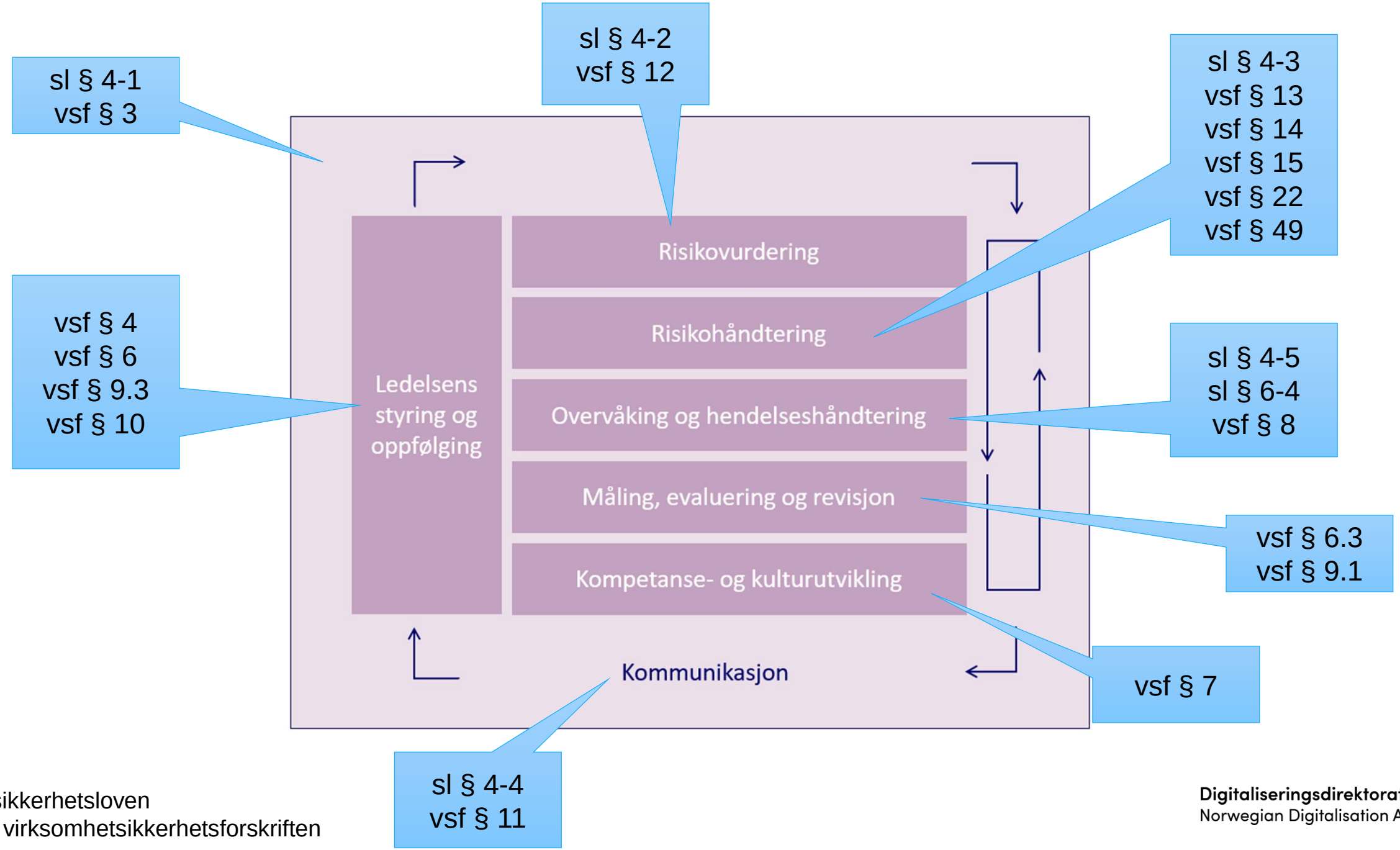


# Digitaliseringsdirektoratet vs DFØ



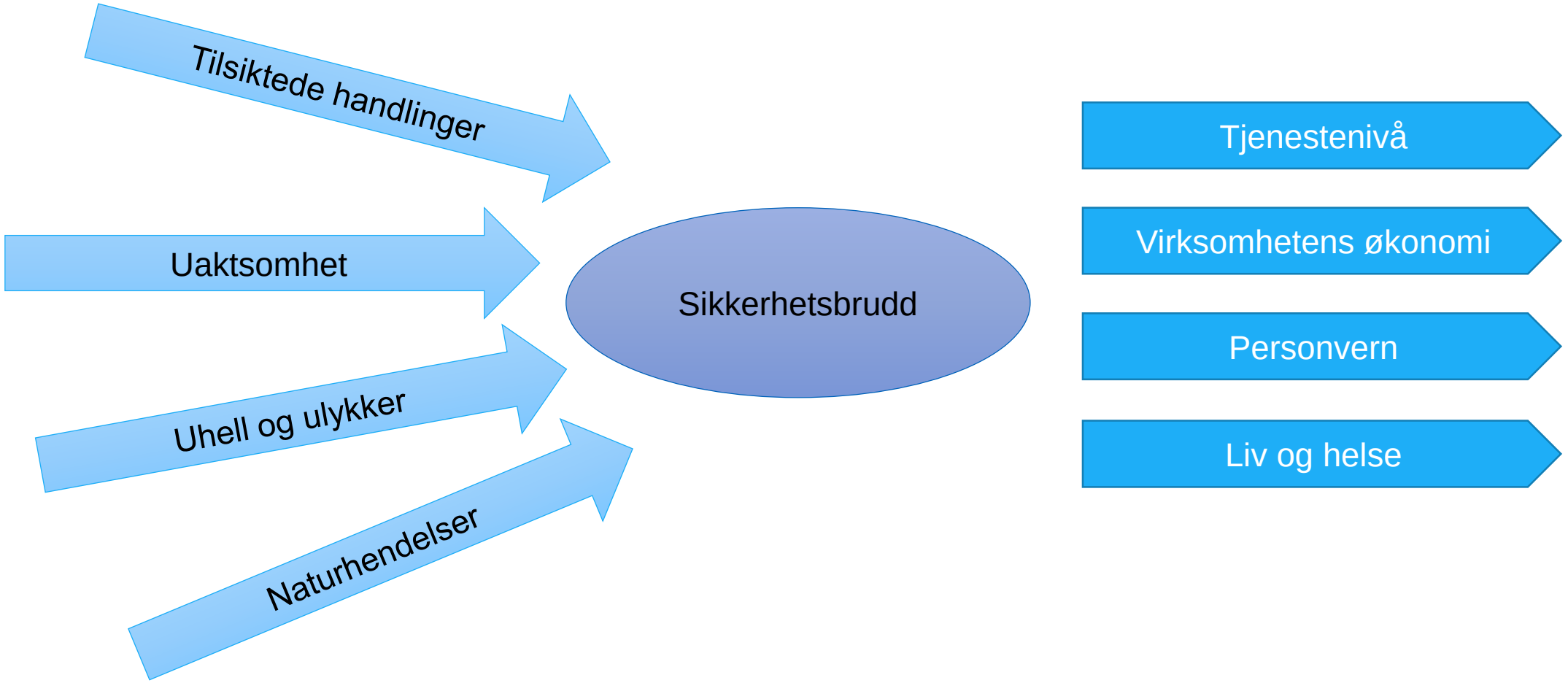



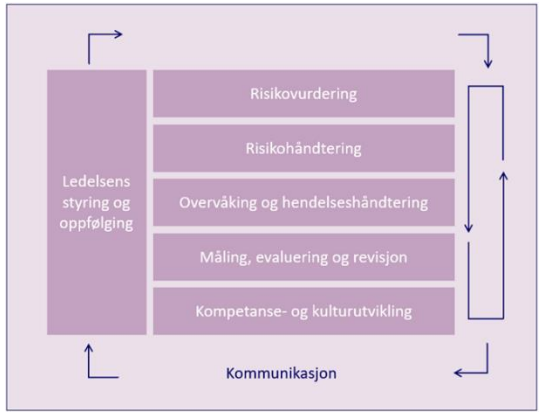


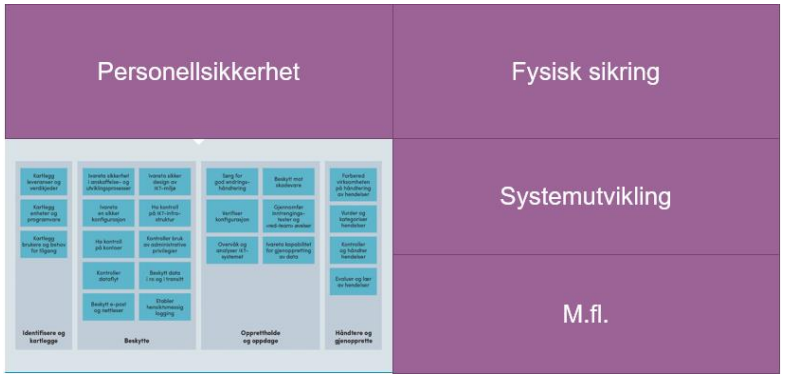

sl = sikkerhetsloven
vsf = virksomhetsikkerhetsforskriften

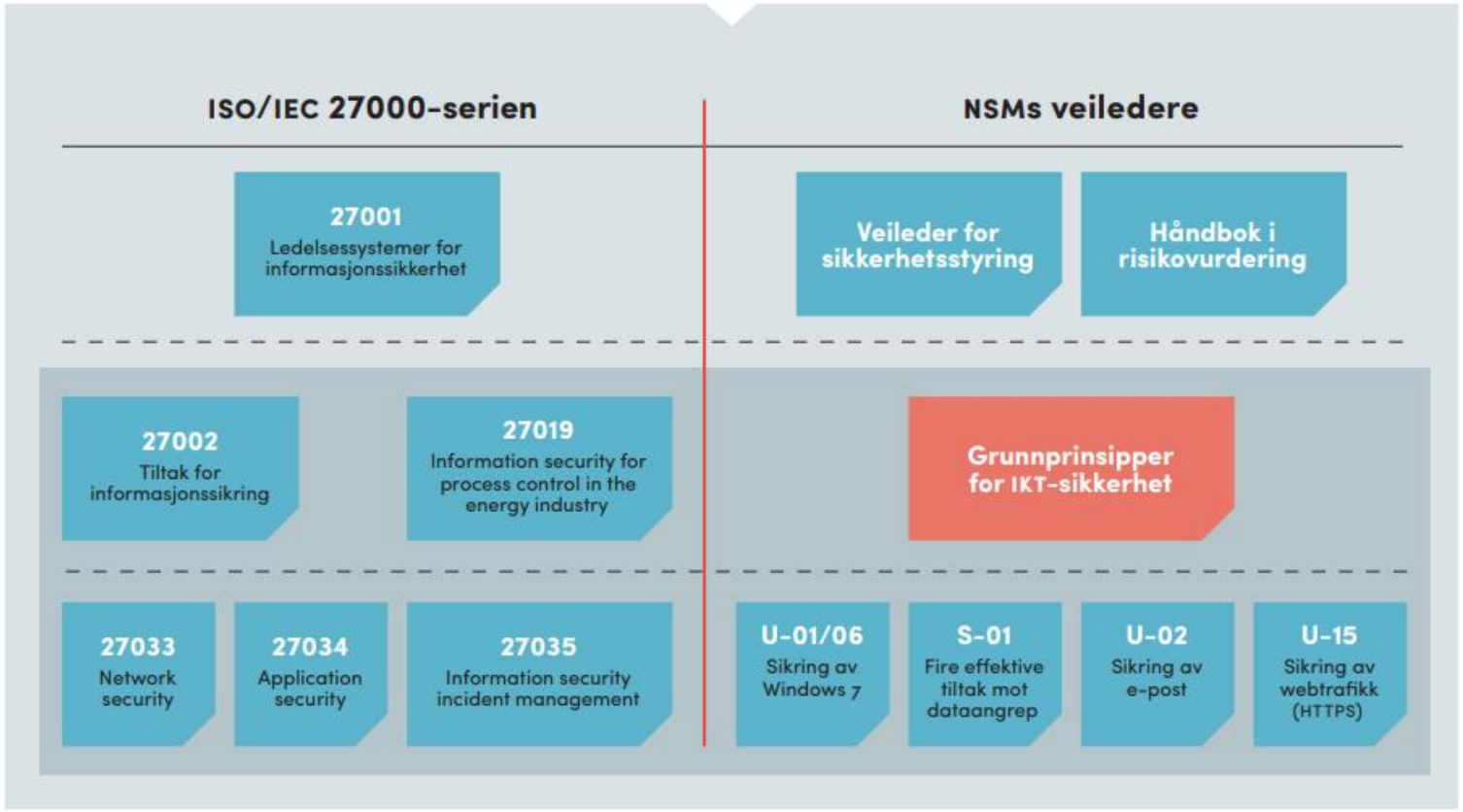
# Kilder

# Konsekvenskategorier




Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon


Personellsikkerhet
Fysisk sikring
Systemutvikling
M.fl.


ISO/IEC 27000-serien
NSMs veiledere
27001
Ledelsessystemer for informasjonssikkerhet
Veileder for sikkerhetsstyring
Håndbok i risikovurdering
27002
Tiltak for informasjonssikring
27019
Information security for process control in the energy industry
Grunnprinsipper for IKT-sikkerhet
27033
Network security
27034
Application security
27035
Information security incident management
U-01/06
Sikring av Windows 7
S-01
Fire effektive tiltak mot dataangrep
U-02
Sikring av e-post
U-15
Sikring av webtrafikk (HTTPS)

# Syv kjennetegn på god internkontroll – interkontroll oppsummert

1

Ledelsesforankret

2

Tilpasset virksomhetens egenart, risiko og vesentlighet

3

Tydeliggjort ansvar, myndighet og rolle

4

Integrert i virksomhetens styring, prosesser og aktiviteter

5

Formalisering og dokumentert, kommunisert og tilgjengeliggjort

6

Etterlevd og systematisk fulgt opp

7

Enhetlig og helhetlig

**Direktoratet for forvaltning og økonomistyring**

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

# Oppsummering og avslutning

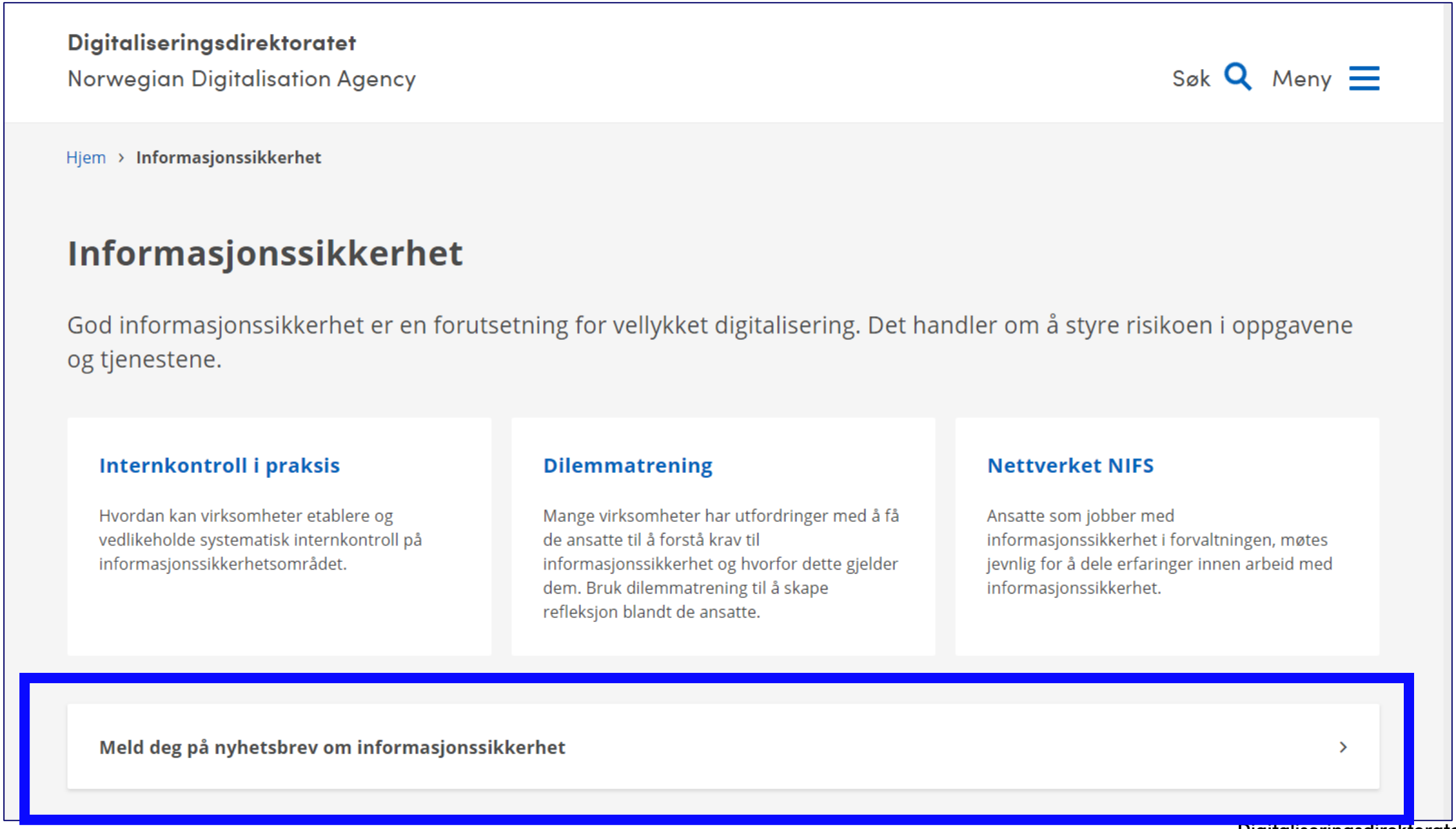
–

Katrine Aam Svendsen
4. februar 2020

# Videre arbeid…

- Oppsummere og bearbeide innspill
- Definere leveranser

- Vil du være med å påvirke arbeidet videre?
  - Meld deg til fokusgruppe!
  - Send e-post til infosikkerhet@digdir.no




https://www.digdir.no/infosikkerhet/882

# Ny e-postadresse

Infosikkerhet@digdir.no

# Digitaliseringskonferansen 2020

- 11. og 12. juni
- Thon Congress Gardermoen


https://sikkerhetsfestivalen.no/

# Neste NIFS-møte

- 22. april
- Tema: Øvelser

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency


www.digdir.no/infosikkerhet/882

infosikkerhet@digdir.no